IAPP.CIPP-E.v2026-06-15.q260

試験コード:	CIPP-E
試験名称:	Certified Information Privacy Professional/Europe (CIPP/E)
認定資格:	IAPP
無料問題数:	260
バージョン:	v2026-06-15
アクセス数:	177
ページビュー数:	2600
https://www.jpnpdf.com/IAPP.CIPP-E.v2026-06-15.q260-mondaishu.html	

最新問題: **1**
次のうち、データ保護責任者の任命が必要となるのはどれですか?
A. 処理は250人以上の従業員を雇用する組織によって実行されます。
B. 処理は、EU 内の個人に営利目的の商品またはサービスを提供する目的で実行されます。
C. The core activities of the controller or processor consist of processing operations of financial information or information relating to children.
D. The core activities of the controller or processor consist of processing operations that require systematic monitoring of data subjects on a large scale.
Answer: D (メーッセージを残す**)**
Reference https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection- regulation-gdpr/accountability-and-governance/data-protection-officers/

最新問題: **2**
シナリオ
次の質問に答えるには、以下を使用してください。
Wonderkidsは、託児サービスのオンライン予約サービスを提供しています。Wonderkidsはフランスに拠点を置いていますが、ウェブサイトはスイスの企業を通じて運営されています。サービスの一環として、Wonderkidsは、提供されたすべての個人データを、自社のシステムを通じて予約された託児サービス提供者に提供します。ウェブサイトで収集される個人データの種類には、託児サービスを予約した人の氏名、住所、連絡先、そして保育を受ける子供の氏名、年齢、性別、健康情報が含まれます。Wonderkidsのウェブサイトのプライバシーに関する声明には、次のように記載されています。
WonderkKidsは、本ウェブサイトを通じてお客様からご提供いただいた情報を、スケジュール管理および健康 ·安全上の理由から、お客様の保育事業者に提供します。また、お客様およびお子様の個人情報を当社の正当な事業目的で使用する場合もあります。また、データの保管にはスイスに所在する第三者ウェブサイトホスティング会社を利用しています。スイスにある機器に保管されるデータは、お客様およびお子様の個人情報の適切な保護を保証するための欧州委員会の規定を満たしています。お客様およびお子様の個人情報は、お客様にとって真に価値のある企業とのみ共有されます。個人情報をご提供いただくことで、お客様は関連企業への情報提供およびプロモーション情報の送付に同意するものとします。

当社は、お客様とお客様のお子様の個人情報を最長 28 日間保持することがあります。その時点でデータは匿名化されます。ただし、お客様の個人情報が 28 日を超えて正当な事業目的で使用される場合は、最長 2 年間保持されることがあります。
当社は、お客様とお子様の個人情報をお客様の同意を得て処理しております。特定の情報をご提供いただけない場合、当社のサービスをご利用いただけない場合があります。お客様には、お客様とお子様の個人情報へのアクセスを要求する権利、お客様とお子様の個人情報を訂正または消去する権利、お客様とお子様の個人情報の訂正または消去を求める権利、お客様とお子様の個人情報の処理に異議を申し立てる権利があります。また、当社のデータ処理活動について監督当局に苦情を申し立てる権利もあります。Wonderkidsはプライバシーステートメントにおいて、どのような追加情報を提供する必要がありますか？
A. ホスティング会社の連絡先情報。
B. データが共有される受信者のカテゴリ。
C. データを保護するための技術的および組織的な対策。
D. プロモーション メールを送信する頻度。
Answer: A (メーッセージを残す**)**

最新問題**: 3**
シナリオ
次の質問に答えるには、以下を使用してください。
ProStorageは、オランダに本社を置く多国籍クラウドストレージプロバイダーです。CEOのルース ･ブラウン氏は、成長のために2本柱の戦略を立てました。1) ProStorageの顧客ベースを世界中に拡大し、2) 効果的なチームを効率的に採用してProStorageの営業部隊を増強することです。この戦略の実行は、ルースの健康状態により、最近、労働時間が制限され、潜在顧客に会うために出張することも困難になったため、複雑になっています。ProStorageの人事部とルースの首席スタッフは現在協力して、彼女のスケジュールを管理し、彼女がすべての医療予約を確実に受けられるようにしています。後者は、ルースが前回インドを旅行した際に健康上の緊急事態に見舞われ、ニューデリーで入院して以来、特に重要になっています。ルースの家族と連絡が取れなかったため、病院はProStorageに連絡し、首席スタッフと連絡を取ることができました。首席スタッフは、人事部長のメアリーと連携していました。
ルースが ProStorage を始めたとき、彼女のリクエストに応じて医師に情報を提供しました。より多くの営業担当者を雇うというルースの戦略目標をサポートするために、人事チームは、新しい従業員の募集、面接、雇用、オンボーディングを効率的に行うためのプロセスの改善に注力しています。これを支援するため、メアリーはドイツを拠点とする HRYourWay とオーストラリアを拠点とする InstaHR という 2 つのベンダーを特定しました。彼女は、ルースと協力して最終決定を下せるよう、両方のベンダーに ProStorage のベンダーリスクレビュープロセスを実行してもらうことにしました。レビュープロセスの一環として、ProStorage のプライバシープログラム (コントローラー BCR の維持とベンダーリスク評価の実施を含む) の保守を担当しているジャッキーは、両方のベンダーをレビューしましたが、移管影響評価は InstaHR についてのみ完了しました。両方のベンダーをレビューした後、彼女は、HRYourWay が最小限のデータ保護オペレーションしか持たない小規模ベンダーであるのに対し、InstaHR はより確立されたプライバシープログラムを誇り、サードパーティの認証を提供しているため、より多くの要件を満たしていると判断しました。
そこで彼女はInstaHRを勧めました。
ProStorageのマーケティングチームは、市場シェア拡大が必要な業界に注力することで、同社の戦略目標の達成にも取り組みました。この取り組みを支援するため、チームは金融業界の顧客と深い関係を持つ米国企業であるUpFinanceをパートナーとして選定しました。ProStorageのデューデリジェンスプロセスにおいて、プライバシーチームのジャッキーは、移転影響評価において、UpFinanceがエンドツーエンドの暗号化（暗号鍵は顧客が保有）を含む複数のデータ保護対策を実施していることを指摘しました。

注目すべきことに、UpFinanceは創業7年間、政府からの要請を一度も受けていません。それでもジャッキーは、UpFinanceが代理で処理する個人データについて政府から要請を受けた場合、当該データを開示する前にProStorageに通知することを契約に盛り込むことを推奨しました。
InstaHR を使用する場合、Jackie はどのような転送メカニズムを推奨しますか?
A. 適切性
B. 拘束力のある企業規則。
C. 従業員の明示的な同意。
D. 標準契約条項
Answer: D (メーッセージを残す**)**
GDPR によれば、第三国または国際機関への個人データの移転は、委員会による十分性の決定、データの輸出者と輸入者による適切な保護措置、または特定の状況に対する特例に基づく必要があります1。このシナリオでは、InstaHR はオーストラリアに拠点を置く会社で、オランダに拠点を置く会社 ProStorage に代わって個人データを処理します。オーストラリアは委員会によって十分なレベルのデータ保護を提供する国として認められていないため2、十分性のオプションは利用できません。拘束的企業準則 (BCR) は、多国籍企業または組織グループが採用する内部規則であり、同じ企業グループ内の個人データを十分なレベルの保護を提供していない国にある事業体に国際的に移転することに関するグローバル ポリシーを定義します3。
ただし、InstaHR は ProStorage と同じ企業グループに属していないため、この場合は BCR は適用されません。従業員の明示的な同意は、特定の状況で例外となる可能性がありますが、自由意志で与えられ、具体的で、情報に基づいた明確なものである必要があり、いつでも撤回できるため、信頼性が高く実用的な転送メカニズムではありません4。したがって、InstaHR を使用するための最も適した転送メカニズムは、標準契約条項 (SCC) です。SCC は、委員会によって事前承認されており、EU/EEA から第三国に個人データを転送する際にデータ保護のための適切な保護手段を提供する契約条項です。SCC はデータ主体によって法的に拘束力があり、執行可能であり、データ輸出者とデータ輸入者の両方に義務を課します。SCC は、GDPR に基づく転送メカニズムとして、データ管理者とデータ処理者によって広く使用されています。参照: 1: Art. 44 GDPR - 転送に関する一般原則22: 十分性決定 - 欧州委員会13: 拘束的企業準則 - 欧州委員会14: GDPR の第 7 条。: 標準契約条項 (SCC) - 欧州委員会1.

最新問題**: 4**
法執行目的での通信トラフィック データの保持は、欧州データ保護法ではどのように扱われていますか?
A. ePrivacy 指令では、個々の EU 加盟国がこのようなデータ保持を行うことが許可されています。
B. ePrivacy 指令は、このようなデータ保持に関する EU 加盟国の規則を調和させます。
C. データ保持指令の廃止により、このようなデータ保持が許可されるようになりました。
D. GDPR では、このようなデータの保持は、犯罪の防止、捜査、検出、または訴追の目的でのみ許可されています。
Answer: (解答を表示する**)**
eプライバシー指令は、電子通信の機密性を保護し、無差別な傍受や監視を防止することを目的とした欧州連合（EU）の指令です。2002年に採択され、2009年に改正されました。インターネットサービスプロバイダー、モバイルネットワーク事業者、オンラインプラットフォームなど、すべての電子通信サービス提供者に適用されます12。
eプライバシー指令の主な目的の一つは、法執行目的での通信トラフィックデータの保持が厳格な条件と保護措置の対象となるようにすることです。通信トラフィックデータとは、IPアドレス、タイムスタンプ、メタデータなど、電子通信の送信またはルーティングに関連するあらゆる情報を指します3。これらのデータは、管轄権を持つ各国当局が犯罪の防止、捜査、摘発、訴追、および国家安全保障の確保のために利用される可能性があります4。

しかし、eプライバシー指令は、EU加盟国が規則を統一することなく、このようなデータ保持を行うことを許可していません。指令第6条(1)(b)は、「加盟国は、トラフィックデータの保持に関して自国が講じるあらゆる措置がこの指令に適合することを確保しなければならない」と規定しています。したがって、各EU加盟国は、指令で定められた要件と制限を遵守する国内法を制定する必要があります12。
データ保持指令（DRD）は、EU加盟国全体で法執行目的で通信トラフィックデータを保持するための共通枠組みを確立することを目指した、以前のEU指令でした。2006年に採択され、2010年に改正されました。しかし、2014年に欧州連合司法裁判所（CJEU）によって手続き上の理由で無効化されました。CJEUは、DRDの一部規定が、個人のプライバシーへの恣意的な干渉から個人を保護する基本権憲章（CFR）第8条第2項など、他のEU指令や原則と矛盾していると判断しました56。
GDPRは、個人データ処理に関する規定を通じてDRDの一部を国内法に組み込むEUの新しい規則です。しかし、法執行目的での通信トラフィックデータの保持という問題には直接的には対処していません。その代わりに、GDPRは、個人データ処理に伴うリスクに見合ったセキュリティレベルを確保するために、プロバイダーに適切な技術的および組織的措置を講じることを義務付けています。これらの措置には、暗号化、仮名化、アクセス制御、アカウンタビリティ7が含まれます。GDPRはまた、個人データへのアクセス、訂正、消去、ポータビリティ、異議申し立てなど、個人データに関する特定の権利を個人に付与しています7。
したがって、現行のEU法では、EU加盟国全体で法執行目的で通信トラフィックデータを保持するための単一の法的根拠は存在しません。各加盟国は、eプライバシー指令で定められた原則と制限を尊重する独自の国内法を制定する必要があります。
参照：
eプライバシー指令
eプライバシー規制
通信トラフィックデータとは何ですか?
通信トラフィックデータはどのように保存されますか?
データ保持指令
データ保持指令がCJEUによって無効化
一般データ保護規則
あなたの個人データに関する権利は何ですか?

最新問題: **5**
GDPR では、データ主体の知らないうちにまたは同意なしに、データ主体の機密性の高い医療情報を収集、使用、開示することが最も許可されないのは誰でしょうか?
A. 問題となっている病状に関連する記事を執筆しているジャーナリストで、そのような情報の公表が公共の利益になると考えている人。
B. データ主体の医療に携わる医療専門家で、データ主体の生命がそのような情報のタイムリーな伝達に左右される場合。
C. データ主体に関わる、またはデータ主体の健康に関する法的紛争の裁定に関与する司法関係者。
D. 公衆衛生を担当する公的機関であり、一般大衆の保護のためにそのような情報を共有することが必要であると考えられる場合。
Answer: D (メーッセージを残す)

最新問題: **6**
主導監督機関 (LSA) の主な懸念事項はプライバシーのどの領域ですか?
A. データ主体の権利
B. データアクセス紛争
C. 国境を越えた処理

D. 特別なデータカテゴリ
Answer: (解答を表示する**)**
説明/参考資料: https://iapp.org/news/a/is-it-possible-to-choose-your-lead-supervisory-authority-under-the-gdpr/

最新問題**: 7**
透明性の原則は、次のどの権利に最も直接関係していますか?
A. 異議申し立ての権利
B. 情報を受ける権利。
C. 忘れられる権利。
D. 処理の制限の権利。
Answer: B (メーッセージを残す**)**
GDPR第5条1項(a)に規定されている透明性原則は、個人データがデータ主体との関係において適法、公正かつ透明性のある方法で処理されることを要求しています。この原則は、GDPR第13条および第14条に規定されている情報提供を受ける権利と密接に関連しています。これらの権利は、管理者に対し、データ主体に対し、個人データの処理に関する特定の情報（管理者の身元および連絡先、処理の目的および法的根拠、個人データの受領者または受領者の区分、データ主体の権利の有無、個人データの保存期間または基準など）を提供することを義務付けています。情報提供を受ける権利は、データ主体が処理の適法性を認識し、検証できるようにし、かつ、データ主体が権利を効果的に行使できるようにすることを目的としています。したがって、透明性原則は情報提供を受ける権利と最も直接的に関連しています。参考文献：
* GDPR第5条(1)(a)
* GDPR第13条
* GDPR第14条
* IAPP CIPP/E 学習ガイド、31ページ

最新問題**: 8**
Murla HB クラブは、新しいアクセス システムをインストールする前に DPIA を実施すべきでした。また、他のどの時期に実施すべきでしたか?
A. 支援者の苦情を受けて
B. 定期的に、新たなリスクが予見された場合
C. シーズン中の各試合の終了時。
D. AEPD による調査の通知後。
Answer: B (メーッセージを残す**)**
GDPR第35条に基づき、データ処理が個人の権利と自由に重大なリスクをもたらす可能性がある場合、データ保護影響評価（DPIA）の実施が義務付けられます。これには、新しい技術を伴う処理、体系的な監視、または機密データの大規模な処理が含まれます。
* DPIA はいつ実施すべきですか?
* 新しい高リスク処理アクティビティ（生体認証アクセス システムなど）を実装する前に。
* リスクに大きな変化が生じたとき (例: セキュリティ更新、規制の変更、新たな脅威)。
* 定期的に新たなリスクを再評価し、軽減します。
* なぜBが正解なのでしょうか?
* DPIA は 1 回限りのプロセスではなく、新しいリスクを評価するために定期的に見直す必要があります。
* 他の回答が間違っているのはなぜですか?

* A (苦情後) # DPIA は事前対策であり、苦情後にのみ行われるものではありません。
* C (シーズン終了時) # GDPR では、評価をイベント サイクルに結び付ける必要はありません。
* D (規制通知後) # DPIA は、対応としてではなく、調査の前に実行する必要があります。
結論: 新たなリスクが発生した場合は、定期的に DPIA を実施する必要があるため、B が正解です。

最新問題: **9**
GDPR では 処理」をどのように定義していますか?
A. 個人データの収集および記録を伴う行為。
B. 個人データまたは個人データ セットに対して実行される任意の操作または操作のセット。
C. データが収集された目的に適合する個人データの使用または開示。
D. 個人データまたは個人データ セットに対して自動化された手段によって実行される操作または操作のセット。
Answer: (解答を表示する**)**
GDPRでは、処理とは 個人データまたは個人データ集合体に対して行われるあらゆる操作または一連の操作（自動的な手段によるか否かを問わず、収集、記録、整理、構造化、保管、適応または変更、検索、照会、使用、送信による開示、頒布またはその他の方法による利用可能化、整合または結合、制限、消去または破棄など）」と定義されています（第4条(2)）。これは、使用される方法や手段に関わらず、個人データに関わるほぼあらゆる活動を網羅する広範な定義です。GDPRではまた、処理は合法、公正、かつ透明性のあるものでなければならないこと、また設計によるデータ保護およびデフォルトのデータ保護の原則を尊重する必要があることも規定しています（第5条）。参考資料 :CIPP/E認定 - 国際プライバシー専門家協会、無料CIPP/E学習ガイド - 国際プライバシー専門家協会、[GDPR - EUR-Lex] これがお役に立てば幸いです。他にご質問がございましたら、お気軽にお問い合わせください。#

最新問題: **10**
Which of the following demonstrates compliance with the accountability principle found in Article 5, Section 2 of the GDPR?
A. Anonymizing special categories of data.
B. Conducting regular audits of the data protection program.
C. Getting consent from the data subject for a cross border data transfer.
D. Encrypting data in transit and at rest using strong encryption algorithms.
Answer: B (メーッセージを残す**)**
The accountability principle found in Article 5, Section 2 of the GDPR requires data controllers to take responsibility for complying with the GDPR and to be able to demonstrate their compliance1. This means that data controllers must implement appropriate technical and organisational measures to ensure and show that they process personal data in accordance with the GDPR2. One of the measures that can demonstrate compliance with the accountability principle is conducting regular audits of the data protection program. Audits are systematic and independent assessments of the data processing activities and the data protection policies and procedures of an organisation3. They can help to identify and address any gaps or risks in the data protection program, as well as to verify the effectiveness and efficiency of the data protection measures3. Audits can also provide evidence of compliance to the supervisory authorities and the data subjects, as well as to enhance the trust and reputation of the organisation3. Therefore, conducting regular audits of the data protection program is a way to demonstrate compliance with the accountability principle.
References: 1: CIPP/E study guide, page 15; Art. 5 GDPR; Accountability principle | ICO2: CIPP/E study guide, page 16; Art. 24 GDPR; [Guide to accountability and governance | ICO]3: CIPP/E study guide, page 91; [Auditing | ICO]; [GDPR Audits: What You Need to Know - IT Governance Blog].

最新問題: **11**
Under which of the following conditions does the General Data Protection Regulation NOT apply to the processing of personal data?
A. When the personal data is processed only in non-electronic form
B. When the personal data is collected and then pseudonymised by the controller
C. When the personal data is held by the controller but not processed for further purposes
D. When the personal data is processed by an individual only for their household activities
Answer: B (メーッセージを残す)
Reference https://gdpr-info.eu/art-6-gdpr/

最新問題: **12**
シナリオ
次の質問に答えるには、以下を使用してください。
ジョーは2000年、米国バーモント州の自宅でグミベア ・カンパニーを設立しました。現在、同社は数十億ドル規模のキャンディ会社に成長し、全大陸で事業を展開しています。同社のITサーバーはすべてバーモント州に設置されています。今年、ジョーは息子のベンを会社に迎え入れ、わずか5年で総売上高を3倍にするという大規模なマーケティング戦略 「プロジェクト ・ビッグ」の責任者に任命しました。ベンは一流大学でコンピュータソフトウェアの博士号を取得しています。ベンは父親の会社に加わることを決めましたが、同時に 「ベン ・ノウズ ・ベスト」という新しいグローバルオンラインデートサイト会社の立ち上げにも密かに取り組んでいます。
ベンは、グミベア ・カンパニーが何百万人もの顧客を抱えていることを認識しており、その多くが理想のパートナーを見つけることに興味を持っているかもしれないと考えています。プロジェクト ・ビッグでは、ベンは同社のオンライン ・ウェブポータルを再設計し、EUおよびその他の地域の顧客に、顧客維持のために追加の個人情報の提供を求めます。プロジェクト ・ベンは、顧客の哲学的信条、政治的意見、婚姻状況に関するデータの収集を開始します。
顧客が独身の場合、ベンはその顧客の個人データをすべてベン ・ノウズ ・ベストの別のデータベースにコピーします。ベンは、顧客一人ひとりに情報提供前にチェックボックスにチェックを入れるよう明確に同意を求めているため、何も悪いことはしていないと考えています。プロジェクト ・ビッグは重要なプロジェクトであるため、ベンの支援のため、コンピューターサイエンスを専攻する大学1年生のサムも採用しています。
ベンが声をかけると、サムはベン ・ノウズ ・ベストのデータベースを見つける。サムは10人の友人とスプリング ・ビーク号でアイルランドへ行く予定なので、アイルランド在住の顧客情報をすべてコピーして、アイルランド滞在中に友人と連絡が取れるようにする。
ジョーは、親友の娘でアメリカのロースクールを卒業したばかりのアリスを、会社の新しい法務顧問として採用しました。アリスはGDPRについて聞いていたので、調べてみました。そしてジョーに近づき、EU域内の事業所から米国への社内データ転送のための法的メカニズムを整備することが会社にとって重要であるため、会社全員が遵守すべき拘束的企業準則（BCR）を起草したと伝えました。
ジョーはアリスの素晴らしい仕事ぶりを高く評価し、米国連邦裁判所で会社に対して提起された大規模な訴訟の処理もアリスに任せると伝えた。訴訟に備えるため、アリスは会社のIT部門に指示し、EUを含む全世界の営業チームのコンピューターのハードドライブのコピーを作成し、全てをアリスに送ってもらい、全員の情報を確認できるようにする。アリスは、自分が第一段階のレビューを担当してくれたことで、ジョーはきっと喜ぶだろうと確信している。なぜなら、これにより、本来であれば外部の法律事務所に支払うはずだった多額の費用を節約できるからだ。
アリスが作成したデータ転送メカニズムは、会社が最初に承認を得ていなかったため、GDPRに違反していますか?
A. 欧州データ保護委員会。

B. 欧州委員会。
C. 欧州連合司法裁判所。
D. データ保護機関。
Answer: D (メーッセージを残す**)**

最新問題**: 13**
DPIA を実施した管理者が監督機関に相談する必要がある可能性が最も高いのはどのような場合ですか?
A. DPIA がビジネス上の利益を保護するために保険が必要となるリスクを特定した場合。
B. DPIA により、個人データを EEA 以外の国に転送する必要があることが判明した場合。
C. DPIA により、提案されている処理によって EU 市民の機密データが収集されることが特定される場合。
D. DPIA により個人の権利と自由に対する高いリスクが特定され、管理者がリスクを軽減するための措置を講じることができる場合。
Answer: D (メーッセージを残す**)**

最新問題**: 14**
GDPR の 個人データ」の定義に含まれない可能性が高いのは次のうちどれですか?
A. フランスに住むアメリカ国民の米国社会保障番号
B. オランダ国民の支払いカード番号
C. イタリアの企業が統計目的で使用したリンクされていない集計データ
D. ドイツの専門試験を受けるドイツ人の受験者の識別番号
Answer: (解答を表示する**)**

最新問題**: 15**
個人データの国際転送に関して、欧州データ保護委員会 (EDPB) は、どのような条件下で例外を適用できると確認しましたか?
A. データ管理者が適切な書類を提出した後、データ保護機関 (DPA) から事前承認を受けている場合。
B. 適切な保護が実行できると判断された場合。
C. データ保護影響評価 (DPIA) で低リスクが示された場合のみ。
D. 最後の手段として、かつ制限的に解釈される場合にのみ使用します。
Answer: (解答を表示する**)**
参考 https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118.pdf (4)

最新問題**: 16**
GDPR では、個人データを収集する前に、データ主体にどのような重要な情報を提供しなければならないのでしょうか?
A. コントローラーがデータを収集する権限と、データが送信される第三者。
B. 関係する政府機関の名前とデータの修正に必要な手順。
C. 管理者の ID と連絡先の詳細、およびデータが収集される理由。
D. コントローラーの連絡先情報と保持ポリシーの説明。
Answer: (解答を表示する**)**
GDPRでは、個人データが収集される際に、データ主体自身または他の情報源から特定の情報を提供することが義務付けられています12。この情報には、管理者 および該当する場合は管理者の代理人およびデータ保護責任者）の身元情報および連絡先、個人データ

の処理目的、および処理の法的根拠が含まれます34。この情報は、個人データの公正かつ透明な処理を確保し、データ主体がGDPRに基づく権利を行使できるようにするために必要です5。
したがって、選択肢Cは、個人データの収集前にデータ主体に提供しなければならない必須情報のうち2つを含んでいるため、正解です。選択肢A、B、Dは、必要な情報がすべて含まれていないか、必須ではない情報が含まれているため、不正解です。参考文献 :1：記事 GDPR 13条 2: GDPR 14条 3: GDPR 13条(1)(a)項 4: GDPR 14条(1)(a)項 5: GDPR 60条 参照: https://gdpr-info.eu/art-13-gdpr/

最新問題**: 17**
シナリオ
次の質問に答えるには、以下を使用してください。
ハビエルさんは、フィットネスクラブEVERFITの会員です。この会社は多くのEU加盟国に支店を持っていますが、GDPRの目的上、主要な事業所はフランスにあります。ハビエルさんは、北アイルランド（英国の一部）のニューリーに住んでおり、国境を越えてアイルランドのダンドークに通勤しています。2年前、出張中に、ハビエルさんはドイツのフランクフルトにあるEVERFITの支店でトレーニング中に写真を撮られました。当時、ハビエルさんは、写真は宣伝目的にのみ使用されると説明され、写真に写ることに同意しました。それ以来、その写真はクラブの英国版パンフレットに使用され、英国版ウェブサイトのランディングページにも掲載されています。しかし、このフィットネスクラブは最近、EU加盟国にあるクラブの様々な支店で会員に対する不当な扱いが蔓延したため、評判が悪くなっています。その結果、ハビエルさんは、自分の写真がフィットネスクラブと公に関連付けられることに不快感を覚えるようになりました。
この件について話し合うため、地元支店の支店長との面談予約を何度も試みたものの、うまくいかなかったハビエルはEVETFITに手紙を送り、ウェブサイトとすべての販促資料から自分の写真を削除するよう要請した。数ヶ月が経過しても、要請に対する返答がなかったハビエルは、この件について強い不安を抱くようになった。他の手段を用いてEVETFITに何度も連絡を取ろうとしたが、それでもうまくいかなかったため、彼はEVETFITに対して訴訟を起こすことを決意した。
ハビエルは、この件について英国情報コミッショナー事務局（ICO、英国の監督機関）に苦情を申し立てました。ICOは、GDPR第56条(3)に基づき、CNIL（EVERFITの主要拠点の監督機関）にこの件を通知しました。EVERFITは英国に拠点を有しているにもかかわらず、CNILはGDPR第60条に基づき、この件を処理することを決定しました。
CNILは、協力手続きに基づき、ICOと連携します。監督当局間の決定における問題を考慮し、欧州データ保護会議が関与し、一貫性メカニズムに基づき拘束力のある決定を下します。
さらに、ハビエルさんは、パンフレットとウェブサイトから自分の写真を削除するという要求をEVERFITが受け入れなかったことによる損害についてEVERFITを訴えている。
協力メカニズムの下で、主導機関（CNIL）は、この問題についての見解を形成した後、何をすべきでしょうか?
A. 他の監督当局に決定案を提出し、意見を求める。
B. 他の監督当局に対し、検討のために決定案を主導当局に提出するよう要請する。
C. 代理監督機関とホスト監督機関のメンバーが共同で決定書を起草するよう要求する。

D. 一貫性メカニズムの有効性を確保するために、決定案を委員会に直接提出します。
Answer: B (メーッセージを残す**)**

最新問題**: 18**
次の状況のうち、個人が処理に対する同意を撤回できる可能性が最も高いのはどれですか?
A. 彼女が現在の銀行を辞めて、別の銀行に移るとき。
B. 最近転職して、同じ会社で働いていなくなったとき。
C. 医師が記録に残した診断結果に彼女が同意できないとき。
D. 組織からマーケティング資料を受け取ることを希望しなくなったとき。
Answer: D (メーッセージを残す**)**
GDPRによれば、同意は個人データ処理の6つの法的根拠の一つです。同意とは、データ主体が自由に、具体的に、十分な情報に基づいて、かつ明確に表明した意思表示であり、データ主体が声明または明確な肯定的行動によって、自己に関する個人データの処理に同意することを意味します。同意はいつでも撤回することができ、撤回は同意を与えるのと同じくらい容易でなければなりません。したがって、個人は組織からマーケティング資料の送付を希望しなくなった場合、処理への同意を撤回することができます。これは個人の明確な意思表示であり、撤回前の同意に基づく処理の合法性に影響を与えないからです。その他の状況は同意とは関係なく、契約、正当な利益、法的義務などの他の法的根拠に関係します。参考：無料CIPP/E学習ガイド、9ページ、CIPP/E認定、3ページ、GDPR、第4条(11)、第6条(1)(a)、第7条(3)。

最新問題**: 19**
シナリオ
次の質問に答えるには、以下を使用してください。
アンナとフランクは二人ともグランチェスター大学で働いています。アンナはデータ保護を担当する弁護士で、フランクは工学部の講師です。大学では様々な種類の記録を保管しています。
* 学生記録には、氏名、学生番号、自宅住所、大学入学前の情報、大学の出席および成績記録、特別な教育ニーズの詳細、財務情報が含まれます。
* 自伝的資料（カリキュラム、専門家の連絡先ファイル、学生の評価、その他の関連する教育ファイルなど）を含むスタッフの記録。
* 卒業生の記録（出身地、生年、入学日、学位授与日など）。
これらの記録は、グランチェスターの卒業生ポータルに登録した卒業生が閲覧できます。
教育省の記録。特定の人口統計グループ（第一世代の生徒など）が平均的にどの程度の進級が見込まれるかを示しています。これらの記録には、氏名や身分証明書番号は含まれていません。
* 大学はセキュリティ ポリシーに従い、転送中および保存中のすべての個人データ記録を暗号化します。
フランクは、教育の質を向上させるため、工学部の学生の成績が教育省の期待値とどの程度一致しているかを調査したいと考えています。彼はアンナのデータ保護に関する研修コースを受講しており、目標達成に必要な範囲を超えて個人データを使用するべきではないことを理解しています。そこで、学生の過去の出身校、当初の成績、現在の成績、初めて進学した大学など、一部のデータのみをエクスポートするプログラムを作成しました。記録は個々の学生レベルで保管したいと考えています。アンナの研修を踏まえ、フランクは学生番号をアルゴリズムにかけ、異なる参照番号に変換します。各記録を継続的に更新できるよう、毎回同じアルゴリズムを使用します。
アンナの業務の一つは、GDPRの要件に従い、処理活動の記録を完了することです。GDPRの要件に従い、アンナからメールによるリマインダーを受け取った後、フランクはアンナにパフォーマンスデータベースについて連絡します。

アンはフランクに、個人データを最小限に抑えるだけでなく、大学は既存データの新たな利用が許容されるかどうかを確認する必要があると説明した。また、GDPRの下では、データ処理を実施する前にリスク分析を実施する必要があるのではないかとも考えている。アンナは追加調査を行った後、フランクとこの件についてさらに話し合う予定だ。
フランクは空き時間に分析作業を行いたいと考え、データを自宅のノートパソコン（暗号化されていない）に転送しました。ところが、大学にノートパソコンを持っていく途中、電車の中で紛失してしまいます。その日、フランクは互換性のある処理について話し合うため、アンナと面会する必要がありました。セキュリティインシデントを報告する必要があるため、同時にアンナにもノートパソコンの紛失について伝えることにしました。
アンナは、この状況ではリスク分析は必要ないと考えるでしょうか?
A. データ対象者はフランクの現在の生徒ではない
B. 処理はデータ主体の権利に悪影響を及ぼさない
C. フランクが処理に使用しているアルゴリズムは技術的に健全である
D. データ主体は、当初の処理に対して明確な同意を与えた
Answer: A (メーッセージを残す**)**
リスク分析とは、組織の個人データ処理活動に影響を及ぼす可能性のある潜在的な脅威と脆弱性を特定、評価、軽減するプロセスです。リスク分析は一度限りの活動ではなく、継続的な監視と更新を必要とする動的なプロセスです。また、リスク分析はGDPRへのコンプライアンスの代替手段ではなく、法的義務とベストプラクティスを特定し、対処することでコンプライアンスを確保するためのツールです。
GDPRによると、組織は、データ主体の権利と自由に高いリスクをもたらす可能性のある、新規または大幅に増加する処理活動を開始する前に、データ保護影響評価（DPIA）を実施する必要があります。DPIAは、そのような処理活動に関連するリスクを特定、評価、軽減することを目的とした、体系的かつ文書化されたプロセスです。DPIAは、管理者（処理の目的と手段を決定する個人または団体）またはその代理人、あるいはその代理人によって実施されなければなりません。
このシナリオでは、フランクは、教育省の期待値に基づき、生徒の成績データを分析するという新たな処理活動について、DPIAを実施しています。この処理活動は、生徒の明示的な同意や認識なしに個人データを収集、保管、使用、転送することを伴うため、生徒の権利と自由にとって大きなリスクとなります。したがって、フランクはこの処理活動を開始する前に、DPIAを実施する必要があります。
ただし、この要件にはいくつかの例外があります。その一つは、処理活動に個人データが含まれ、その個人データが当初の収集目的またはその他の処理目的とはもはや関連がない場合です。この場合、フランクは、既存の個人データが新たな目的に適切かつ関連性があり、必要な範囲に限定されていることを保証できる限り、DPIAを実施することなく既存の個人データを使用することができます。
したがって、この状況では、データ主体がフランクの現在の生徒ではなくなった限り、アンナはリスク分析は不要であると判断するでしょう。つまり、フランクは、既存の生徒記録が適切かつ関連性があり、新しい目的に必要なものに限定されていることを保証できる限り、DPIAを実施することなく既存の生徒記録を使用することができます。
参考文献:
* リスクとデータ保護影響評価（DPIA）| ICO
* GDPR リスク評価とは何ですか? なぜ重要なのですか?
* GDPRコンプライアンスリスク評価のベストプラクティス | Accountable
* GDPRコンプライアンスにリスク評価が不可欠な理由

最新問題**: 20**
シナリオ

次の質問に答えるには、以下を使用してください。
Wonderkidsは、託児サービスのオンライン予約サービスを提供しています。Wonderkidsはフランスに拠点を置いていますが、ウェブサイトはスイスの企業を通じて運営されています。サービスの一環として、Wonderkidsは、提供されたすべての個人データを、自社のシステムを通じて予約された託児サービス提供者に提供します。ウェブサイトで収集される個人データの種類には、託児サービスを予約した人の氏名、住所、連絡先、そして保育を受ける子供の氏名、年齢、性別、健康情報が含まれます。Wonderkidsのウェブサイトのプライバシーに関する声明には、次のように記載されています。
WonderkKidsは、本ウェブサイトを通じてお客様からご提供いただいた情報を、スケジュール管理および健康 ･安全上の理由から、お客様の保育サービス提供者に提供します。また、お客様およびお子様の個人情報を当社の正当な事業目的で使用する場合があり、データの保管にはスイスに所在する第三者ウェブサイトホスティング会社を利用しています。スイスに所在する機器に保管されるデータは、お客様およびお子様の個人情報の適切な保護を保証するための欧州委員会の規定を満たしています。
当社は、お客様とお子様の個人情報を、お客様に真の価値を提供できると判断する企業とのみ共有いたします。個人情報をご提供いただくことで、お客様は、関連企業への情報提供およびプロモーション情報の送付に同意するものとします。
当社は、お客様とお客様のお子様の個人情報を最長 28 日間保持することがあります。その時点でデータは匿名化されます。ただし、お客様の個人情報が 28 日を超えて正当な事業目的で使用される場合は、最長 2 年間保持されることがあります。
当社は、お客様およびお子様の個人情報をお客様の同意を得て処理しております。特定の情報をご提供いただけない場合、当社のサービスをご利用いただけない場合があります。お客様には、お客様およびお子様の個人情報へのアクセスを要求する権利、お客様またはお子様の個人情報を訂正または消去する権利、お客様および/またはお子様の個人情報の訂正または消去を求める権利、お客様およびお子様の個人情報の処理に異議を申し立てる権利があります。また、当社のデータ処理活動について監督当局に苦情を申し立てる権利もあります。WonderKidsとホスティングサービスプロバイダー間の契約には、どのような内容を含める必要がありますか？
A. データを保護するための技術的および組織的な対策を実施する要件。
B. コントローラー間モデル契約条項。
C. データ主体の監査権限。
D. 秘密保持契約。
Answer: A (メーッセージを残す**)**
GDPR（一般データ保護規則）は、EU居住者の個人データを処理するすべての組織に適用されます。処理場所の如何に関わらず適用されます。したがって、フランスに拠点を置くデータ管理者であるWonderKidsは、WonderKidsに代わってデータ処理者として機能しているスイスのホスティングサービスプロバイダーに個人データを転送する際に、GDPRを遵守する必要があります。
GDPR第28条に基づき、データ管理者は、データ主体の権利保護とデータのセキュリティを確保するために、適切な技術的および組織的措置を実施する十分な保証を提供するデータ処理者のみを利用しなければなりません。また、データ管理者とデータ処理者は、処理の対象、期間、性質、目的、ならびにデータ管理者の義務と権利を規定した書面による契約またはその他の法的行為を締結しなければなりません。
契約には、とりわけ以下の規定を含める必要があります。
* データ処理者は、EU または加盟国の法律で義務付けられている場合を除き、第三国または国際機関への個人データの転送を含め、データ管理者からの文書化された指示に従ってのみ個人データを処理する必要があります。
* データ処理者は、個人データを処理する権限を与えられた者が機密保持を約束しているか、または適切な法的機密保持義務を負っていることを保証する必要があります。
* データ処理者は、処理のセキュリティに関連する GDPR の第 32 条に従って必要なすべての措置を講じる必要があります。

* データ処理者は、他の処理者を雇用するための条件を尊重し、他の処理者の追加または置き換えに関する変更を予定している場合はデータ管理者に通知し、データ管理者にそのような変更に異議を申し立てる機会を与えなければなりません。
* データ処理者は、処理のセキュリティ、個人データ侵害の通知、個人データ侵害のデータ主体への伝達、データ保護影響評価、監督当局との事前協議に関連する、GDPR の第 32 条から第 36 条に従った義務の遵守を保証するためにデータ管理者を支援する必要があります。
* データ処理者は、データ管理者の選択により、処理に関連するサービスの提供終了後にすべての個人データを削除するかデータ管理者に返却し、EUまたは加盟国の法律で個人データの保管が義務付けられていない限り、既存のコピーを削除する必要があります。
* データ処理者は、GDPR 第 28 条に規定された義務の遵守を証明するために必要なすべての情報をデータ管理者に提供し、データ管理者またはデータ管理者が義務付けた別の監査人が実施する検査を含む監査を許可し、これに協力する必要があります。
したがって、4 つのオプションのうち、WonderKids とホスティング サービス プロバイダー間の契約に含める必要があるのは、データを保護するための技術的および組織的対策を実施するという要件です。これは、GDPR の第 28 条および第 32 条に基づくデータ処理者の義務の一部です。
その他の選択肢はGDPRでは必須ではありませんが、状況によっては推奨または望ましい場合があります。コントローラー間モデル契約条項は、個人データがデータコントローラーからデータプロセッサーへではなく、あるデータコントローラーから別のデータコントローラーへ転送される場合に使用されます。
GDPRではデータ主体の監査権は明示的に要求されていませんが、データ管理者は、データ処理者がデータ管理者またはデータ管理者が委託した他の監査人による監査を許可し、その監査に協力することを確保する必要があります。秘密保持契約は個人データの機密性を保護する上で有用ですが、データ処理関係のあらゆる側面を網羅しているわけではないため、GDPRの遵守を確保するには不十分です。
参考文献:
GDPR
ウェブホスティングとGDPRコンプライアンス - 注目すべき点
GDPR: サードパーティサービスプロバイダーのセキュリティを確認する必要がある理由 サードパーティサービスプロバイダーのGDPRコンプライアンス: ベンダー管理

最新問題**: 21**
英国は、ブレグジットの規定に基づきEUを離脱した後、十分性認定を求めることになります。その理由は何ですか？
A. 保険長官は、データ保護法により適切性の判断が必要であると判断しました。
B. 加盟国が EU を離脱すると、適格性の決定は自動的に失効します。
C. 英国は GDPR の対象外となったため、第三国となりました。
D. 英国はEUに加盟していないため、信頼性が低下しています。
Answer: C (メーッセージを残す**)**
GDPRは、EU域内に所在する管理者または処理者の活動に関連する個人データの処理に適用されます。処理がEU域内で行われるか否かは関係ありません。また、GDPRは、EU域内に所在しない管理者または処理者による、EU域内に所在するデータ主体の個人データの処理にも適用されます。この場合、処理活動は、EU域内の当該データ主体への商品またはサービスの提供、またはEU域内で行われる当該データ主体の行動の監視に関連するものとなります1。したがって、Brexitの規定によりEUを離脱した後、英国はGDPRの目的において第三国となり、EUから英国への個人データの移転は、GDPR第5章に基づく国際データ移転に関する規則の対象となります2。EUと英国間のデータフローの継続性と安定性を確保するため、英国は欧州委員会に対し、第三国がEUと同等のデータ保護水準を提供していることを正式に認める十分性認定を申請しました3。2021年6月28日、欧州委員会は英国に関する2つの十分性認定を

採択しました。1つはGDPRに基づく移転に関するもので、もう1つは法執行指令（LED）に基づく移転に関するものです4。これらの認定により、EUから英国への個人データの自由な流通が認められ、追加の保護措置は必要なく、修正、停止、または早期に廃止されない限り、2025年6月27日まで有効となります5。参考：
GDPR第3条
GDPR、第5章
EU 域外諸国のデータ保護の適切性、「適切性決定」セクション 英国政府は、欧州委員会のデータ保護の適切性決定草案を歓迎 適切性、「EU GDPR の適切性決定には何が書かれているか」セクション

最新問題: **22**
次のどれがクラウド コンピューティング サービスの共通の特性として認識されていませんか?
A. サービスのインフラストラクチャはサプライヤーの顧客間で共有され、複数の国に配置される場合があります。
B. サプライヤーは、処理に適用される場所、セキュリティ対策、およびサービス基準を決定します。
C. サプライヤーは、容量に応じて顧客データをインフラストラクチャ内で転送することを許可します。
D. サプライヤーは、サプライヤーによって処理されるデータに関連するベンダーのビジネスリスクを負います。
Answer: (解答を表示する**)**
これはクラウドコンピューティングサービスに共通する特徴ではありません。なぜなら、サプライヤーは通常、ベンダーの事業リスクを負わないからです。実際、サプライヤーはデータ漏洩や損失に対する責任を制限することが多く、ベンダーはデータ保護に関する法令遵守の責任を負います。その他の選択肢は、クラウドコンピューティングが柔軟で拡張性が高く、費用対効果の高いデータ処理方法であるという性質を反映している一方で、データ保護とセキュリティの面で課題も抱えているため、クラウドコンピューティングサービスの一般的な特徴です。参考文献：
* 無料のCIPP/E学習ガイド、17ページ、セクション2.3.2
* CIPP/E認証、12ページ、セクション2.3.2
* Cipp-e 学習ガイド、授業ノートと要約、23 ページ、セクション 2.3.2
参考: https://www.softwaremajor.com/news-articles/64-gdpr-how-does-it-apply-to-the-cloud

最新問題: **23**
EUの管理者が、処理者を介して個人データを第三国に移転することを計画しています。EDPB意見22/2024によれば、推奨される最初のステップは何ですか？
A. プロセッサとの適切な安全対策を特定します。
B. プロセッサへの転送の法的根拠を確認します。
C. 転送マッピングがプロセッサによって実行されることを確認します。
D. プロセッサに関する移転影響評価を実施します。
Answer: C (メーッセージを残す**)**
EDPB 勧告 01/2020 (更新され、後に意見 22/2024 に組み込まれた) によれば、国際転送の最初のステップは 転送を把握すること」です。これは、プロセッサまたはサブプロセッサを介して行われたものも含め、個人データの第三国へのすべての転送をマッピングすることを意味します。
論理は次のとおりです。
* ステップ 1 - 転送のマッピング: 個人データが EEA から出ていくかどうか、またどのエンティティ (コントローラー、プロセッサー、またはサブプロセッサー) を経由して出ていくかを特定し、文書化します。

* ステップ 2 - 転送ツールの検証: 転送が適切性、SCC、BCR、または特例に依存しているかどうかを確認します。
* ステップ 3 - 第三国の法律を評価する (TIA): 移転マッピングの後にのみ、移転影響評価を実施します。
* ステップ 4 - 補足的措置:必要に応じて、技術的、契約的、または組織的な保護手段を採用します。
したがって、EDPB ガイダンスに沿って推奨される最初のステップは、転送マッピング (オプション C) です。
#参考：補足的移転措置に関するEDPB勧告01/2020、ステップ1 「移転について知る」、CIPP/E教科書（第3版）、第12章 「国際データ移転」。

最新問題**: 24**
英国は、Brexit の規定に従って EU を離脱した後、十分性認定を求めることになる。
その理由は何でしょうか?
A. 保険長官は、データ保護法により適切性の判断が必要であると判断しました。
B. 加盟国が EU を離脱すると、適格性の決定は自動的に失効します。
C. 英国は GDPR の対象外となったため、第三国となりました。
D. 英国はEUに加盟していないため、信頼性が低下しています。
Answer: C (メーッセージを残す**)**
GDPRは、EU域内に所在する管理者または処理者の活動に関連する個人データの処理に適用されます。処理がEU域内で行われるか否かは問いません。また、GDPRは、EU域内に所在しない管理者または処理者による、EU域内に所在するデータ主体の個人データの処理にも適用されます。この場合、処理活動は、EU域内のデータ主体への商品またはサービスの提供、またはEU域内で行われる限りにおけるその行動の監視に関連するものとなります1。したがって、Brexitの規定によりEUを離脱した後、英国はGDPRの目的において第三国となり、EUから英国への個人データの移転は、GDPR第5章に基づく国際データ移転に関する規則の対象となります2。EUと英国間のデータフローの継続性と安定性を確保するため、英国は欧州委員会に対し、第三国がEUと同等のデータ保護水準を提供していることを正式に認める十分性認定を求めました3。2021年6月28日、欧州委員会は英国に関する2つの十分性認定を採択しました。1つはGDPRに基づく移転に関するもので、もう1つは法執行指令（LED）4に基づく移転に関するものです。これらの認定により、EUから英国への個人データの自由な流通が可能となり、追加の保護措置は不要となります。これらの認定は、早期に修正、停止、または廃止されない限り、2025年6月27日まで有効となる予定です5。参考文献：
* GDPR第3条
* GDPR、第5章
* EU域外諸国におけるデータ保護の適切性、「適切性決定」セクション
* 英国政府は欧州委員会のデータ妥当性に関する決定案を歓迎
* 適切性、「EU GDPR の適切性決定には何が述べられているか」セクション
参考：https://www.euractiv.com/section/digital/news/commission-must-refuse-uk-data-adequacy-rights- group-says/

最新問題**: 25**
欧州人権条約（ECHR）第8 条に基づくプライバシーの権利を考慮する場合、正しい記述はどれですか。
A. プライバシーの権利は絶対的な権利である
B. プライバシーの権利は、欧州人権条約に基づく他の権利とバランスをとる必要がある。
C. 欧州人権条約第10条に基づく表現の自由の権利は、常にプライバシーの権利よりも優先される。
D. プライバシーの権利は、意見を持ち、干渉されることなくアイデアを受け取ったり伝えたりする権利を保護します。
Answer: B (メーッセージを残す**)**

欧州人権条約第 8 条は、私生活、家族生活、住居、通信の尊重の権利を保護しています。
しかし、この権利は絶対的なものではなく、法律に基づき、正当な目的のために公的機関によって制限される可能性があります。欧州人権裁判所（ECtHR）は、このような制限が正当かどうかを判断するための2段階のテストを開発しました。第1に、裁判所は、国家安全保障、公共の安全、犯罪防止など、公的機関が追求する正当な目的があるかどうかを審査する必要があります。第2に、裁判所は、比例性、必要性、より制限の少ない代替手段など、関連するすべての要素を考慮に入れ、公的機関が使用する手段がその目的を達成するために適切かつ必要であるかどうかを評価する必要があります12。したがって、プライバシーの権利は絶対的な権利ではなく、ECHRに基づく他の権利とのバランスをとる必要がある限定的な権利です。参考文献：
* 第8条 - 個人データの保護
* 私生活と家族生活を尊重される権利
* 私生活および家族生活を尊重される権利
* 欧州人権条約第8条に関するガイド
* 欧州人権条約 - 第8条
参考：https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf (15)

最新問題**: 26**
GDPR では、データ主体の知らないうちにまたは同意なしに、データ主体の機密性の高い医療情報を収集、使用、開示することが最も許可されないのは誰でしょうか?
A. データ主体に関わる、またはデータ主体の健康に関する法的紛争の裁定に関与する司法関係者。
B. 公衆衛生を担当する公的機関であり、一般大衆の保護のためにそのような情報を共有することが必要であると考えられる場合。
C. データ主体の医療に携わる医療専門家で、データ主体の生命がそのような情報のタイムリーな伝達に左右される場合。
D. 問題となっている病状に関連する記事を執筆しているジャーナリストで、そのような情報の公表が公共の利益になると考えている人。
Answer: B (メーッセージを残す**)**
説明/参考資料: https://www.eui.eu/Documents/ServicesAdmin/DeanOfStudies/ResearchEthics/Guide-Data- Protection-Research.pdf

最新問題**: 27**
データ侵害によって生じるリスクのレベルを評価する際に、考慮する必要がないのは次のどれですか?
A. 個人の識別の容易さ。
B. 関係するデータ プロセッサのサイズ。
C. データ コントローラーの特殊な特性。
D. 個人データの性質、機密性、量。
Answer: B (メーッセージを残す**)**
データ侵害によって生じるリスクのレベルを評価する際に、関与するデータ処理者の規模を考慮する必要はありません。GDPRによれば、データ侵害とは「送信、保管、またはその他の方法で処理された個人データの偶発的または違法な破壊、紛失、改ざん、不正開示、またはアクセスにつながるセキュリティ侵害」です1。GDPRは、データ管理者およびデータ処理者に対し、データ侵害が自然人の権利と自由にリスクをもたらす可能性が低い場合を除き、72時間以内に関連監督機関にデータ侵害を通知することを義務付けています2。また、GDPRは、データ侵害がデータ主体の権利と自由に高いリスクをもたらす可能性がある場合、データ管理者に対し、影響を受けるデータ主体にデータ侵害を遅滞なく通知することを義務付けています3。

GDPRはリスクレベルを判断するための具体的な基準を明示していませんが、前文85において「データ主体の権利と自由に対するリスクの可能性と重大性は、処理の性質、範囲、状況、目的を参照して判断されるべきである」という指針を示しています。また、前文では、個人の識別の容易さ、個人データの特殊なカテゴリ、処理の大規模さ、データ管理者の特殊な特性など、リスクを高める可能性のある要因についても言及しています。したがって、データ侵害によって生じるリスクレベルを評価する際には、これらの要因を考慮する必要があります。
ただし、関係するデータ処理者の規模は、データ侵害がデータ主体に与える影響に影響を与えないため、リスク評価には関係ありません。データ処理者は、データ管理者に代わって個人データを処理する責任のみを負い、データ主体とは直接の関係がありません。データ侵害が発生した場合のデータ処理者の義務は、データ管理者に遅滞なく通知し、データ管理者が GDPR に基づく義務を遵守できるよう支援することです。データ処理者の規模は、これらの義務を履行する能力に影響を与える可能性がありますが、データ侵害自体によって生じるリスクのレベルは変わりません。参考 : 1 :GDPR 第 4 条 (12) 2 :GDPR 第 33 条 3 :GDPR 第 34 条 : GDPR の 85 番目の説明 : GDPR 第 4 条 (8) : GDPR 第 28 条 これがお役に立てば幸いです。他にご質問がございましたら、お気軽にお問い合わせください。

最新問題: **28**
データ保護に関する欧州モデルを最もよく表す用語は何ですか?
A. セクター別
B. 自主規制
C. 市場ベース
D. 包括的
Answer: (解答を表示する)
参考 :https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf

最新問題: **29**
あるオンライン企業は、多岐にわたるサービスを提供しているため、プライバシーに関する取り組みも多岐にわたります。全てを説明するとポリシーが分かりにくくなるという懸念に対し、どのように対処するのが最善でしょうか？
A. 処理活動に関する一般的な情報のみを提供し、詳細情報についてはフリーダイヤル番号を提供します。
B. サイトにアクセスすることで訪問者がプライバシー ポリシーと利用規約に同意することを規定するバナーを Web サイトに掲載します。
C. ウェブサイトや電子メールでのコミュニケーションで階層化されたプライバシー通知を使用します。
D. データ主体に郵送されるプライバシー通知でデータの使用を特定します。
Answer: (解答を表示する)

最新問題: **30**
データ処理者を雇う場合、セキュリティ侵害が発生した場合に責任を回避するためにデータ管理者が頼ることができないアクションはどれですか?
A. 契約前の段階で実施されたデューデリジェンスの手順を文書化します。
B. リスク評価を実施して、アウトソーシングの潜在的な脅威を分析します。
C. プロセッサが適切な監督機関に直接通知することを要求します。
D. プロセッサが市場で入手可能な最良の選択肢であったという証拠を維持します。
Answer: (解答を表示する)

GDPRは、データ管理者がデータ処理者に個人データ処理を委託する際に、いくつかの義務を課しています。これらの義務の一つは、管理者と処理者との間の契約またはその他の法的行為において、処理者がGDPRに基づく義務の遵守において管理者を支援することを確実にすることであり、これには個人データ侵害を管轄監督当局、および該当する場合は影響を受けるデータ主体に通知する義務が含まれます1。しかし、これは処理者が管理者の関与なしに監督当局に直接通知できることを意味するものではありません。GDPRは、管理者が監督当局に遅滞なく、そして可能であれば侵害を認識してから72時間以内に通知する責任があることを明確に規定しています2。処理者は、侵害を認識した後、遅滞なく管理者に通知する必要があります3。したがって、処理者に適切な監督当局への直接通知を要求することは、データ管理者がセキュリティ侵害発生時の責任を回避するために頼りにできる措置ではありません。なぜなら、それはGDPRおよび管理者自身の義務に反するからです。オプションA、B、Dは、データ管理者がデューデリジェンスを実施し、アウトソーシングの潜在的な影響を評価し、信頼性が高くコンプライアンスに準拠した処理者を選択したことを示すため、責任リスクを軽減するために実施できる措置です。参考文献 :1 :GDPR第28条(3)(f) 2 :GDPR第33条(1) 3 :GDPR第33条(2)

最新問題**: 31**
GDPRでは、管理者はデータ主体に対し、データの処理に関する詳細な情報を提供することが義務付けられています。管理者がデータ主体から直接データを取得する場合、以下の情報のうち、法的に提供する必要がないものはどれですか？
A. 受信者または受信者のカテゴリ。
B. 関係する個人データのカテゴリ。
C. アクセス、消去、制限、移植性の権利。
D. 監督機関に苦情を申し立てる権利。
Answer: B (メーッセージを残す**)**
GDPR第13条によれば、管理者がデータ主体から直接個人データを取得する場合、管理者はデータ主体に対し、データ処理に関する一定の情報（管理者の身元および連絡先、処理の目的および法的根拠、受領者または受領者の区分、保管期間、データ主体の権利、苦情申し立て権など）を提供しなければならない。ただし、データ主体は自らデータを提供したため、当該個人データの区分については既に把握しているため、管理者はデータ主体に当該個人データの区分を提供する必要はない。これは、管理者がデータ主体以外の情報源から個人データを取得する場合に適用される第14条とは異なり、管理者はデータ主体に対し、当該個人データの区分およびデータの情報源を通知する必要がある。参考文献：
* GDPR第13条 - データ主体から個人データが収集される場合に提供される情報
* GDPR第14条 - 個人データがデータ主体から取得されていない場合に提供される情報
* 第13条: データ主体から個人データを収集する場合に提供される情報 - GDPR

最新問題**: 32**
マーケティング担当者が EU 内の消費者に電子メール マーケティング メッセージを送信するには、どのような許可が必要ですか?
A. 既に顧客でない限り、消費者に対する事前のオプトイン同意。
B. 消費者が電子メール マーケティングの受信に同意することを示す、事前にチェックされたボックス。

C. 消費者の電子メール アドレスがマーケティング目的で使用されることを通知します。
D. 事前の許可は必要ありませんが、消費者に送信されるすべての電子メールでオプトアウトが必要です。
Answer: (解答を表示する**)**
参考 :https://www.forbes.com/sites/forbescommunicationscouncil/2018/06/27/what-gdpr-means-for- email-marketing-to-eu-customers/#64020aa8374a

最新問題**: 33**
クッキーの合法的な適用のためにブラウザ設定に依拠できるのはどのような場合ですか?
A. ユーザーが厳密に必要な Cookie を拒否した場合。
B. ユーザーが設定を調整できることを認識している場合。
C. 設定されている Cookie に関する情報がユーザーに提供される場合。
D. ユーザーがブラウザ設定で行った選択を回避できない場合。
Answer: D (メーッセージを残す**)**
クッキーおよび類似のテクノロジーの使用に関する ICO ガイダンス1 によれば、ブラウザ設定やその他の制御メカニズムは、以下の条件を満たす場合にのみ、クッキーの合法的な適用に依拠できます。
* ユーザーのプライバシーを保護し、Cookie や類似のテクノロジーの使用を制御できるように設計されています。
* 目立つようになっており、使いやすく、ユーザーに不要な手順の実行や不要な情報の提供を求めません。
* クッキーや類似のテクノロジーのさまざまなタイプや目的に対するユーザーの好みを表現できるほど具体的かつ詳細です。
* 設定またはアクセスされる Cookie や類似のテクノロジー、およびそれらが使用される目的について十分な情報と理解を得ていること。
* 使用される Cookie や類似のテクノロジー、またはその使用目的の変更を反映するために、定期的に確認および更新されます。
* ユーザーの選択を妨げる可能性のある他のソフトウェアまたは設定によって上書きまたは回避されないこと。
* いつでも同意を撤回できる効果的な手段を提供します。
したがって、ブラウザ設定やその他の制御メカニズムは、Cookieや類似のテクノロジーに対する同意を得るための有効な手段となり得ますが、それはこれらの高い基準を満たし、ユーザーがデバイス上でCookieや類似のテクノロジーを利用する上で現実的かつ有意義な選択肢を持つことを保証する場合に限られます。参考文献 :1. Cookie規則への準拠方法 | ICO。4 アクセス日 :2023年12月11日）。

最新問題**: 34**
多国籍企業が、ヨーロッパに拠点を置く従業員を含むすべての現従業員および潜在的な従業員に対して身元調査を実施したい場合、その企業はどのような重要な規定に従う必要がありますか?
A. 従業員の身元調査は、すべての従業員に事前に通知した場合にのみ実行できます。
B. 身元調査は、ヨーロッパに拠点を置く従業員を含むすべての従業員からの事前の通知と明示的な同意がある場合にのみ許可されます。
C. 欧州の従業員に対する身元調査は、データ保護法と雇用法に基づいて行われますが、加盟国によって異なる場合があります。
D. ヨーロッパの従業員に対する身元調査は許可されない可能性がありますが、企業は正当な利益に基づいてリストを作成し、雇用に不適格な個人を特定することができます。
Answer: C (メーッセージを残す**)**

GDPRは身元調査を明確に規制していませんが、身元調査中に取得または使用される可能性のある個人データの処理には適用されます。したがって、企業は、合法性、公平性、透明性、データの最小化、目的の限定、正確性、保存期間の制限、完全性と機密性、説明責任といったGDPRの原則を遵守する必要があります。また、企業は、法的義務、正当な利益、同意など、個人データを処理する法的根拠を特定し、情報開示、アクセス、訂正、消去、制限、異議申し立て、ポータビリティといったデータ主体の権利を尊重する必要があります。さらに、企業は、GDPR第10条および各加盟国の法律の対象となる、特別なカテゴリーのデータ（生体認証データ、健康データ、政治データなど）や、犯罪歴や犯罪行為に関連するデータの処理に関する具体的な規則や制限を認識しておく必要があります。企業はまた、身元調査の範囲、方法、目的に追加の条件や制限が課される可能性のある、各国の雇用法および関連監督当局のガイドラインも考慮する必要があります。例えば、一部の加盟国では、身元調査を実施する前に、監督機関、データ主体、または労働組合への事前の承認、通知、または協議が必要となる場合があります。また、一部の加盟国では、ソーシャルメディアスクリーニング、信用調査、犯罪歴調査など、特定の職種または業種において必要かつ適切で関連性のある場合を除き、特定の種類の身元調査を禁止または制限する場合があります。したがって、企業は、事業を展開または従業員を採用する各加盟国における法的枠組み、身元調査のリスクとベネフィットを徹底的に評価し、GDPRに準拠した方法で身元調査を実施するための明確で一貫した方針と手順を確立する必要があります。参考資料 :GDPRに基づく「身元調査」の方法、GDPRに準拠した身元調査の実施方法、欧州におけるGDPRと犯罪歴データの処理、雇用前審査 :データ保護と犯罪歴、GDPRが身元調査に与える影響

最新問題**: 35**
SCENARIO
Please use the following to answer the next question:
Anna and Frank both work at Granchester University. Anna is a lawyer responsible for data protection, while Frank is a lecturer in the engineering department. The University maintains a number of types of records:
Student records, including names, student numbers, home addresses, pre-university information, university attendance and performance records, details of special educational needs and financial information.
Staff records, including autobiographical materials (such as curricula, professional contact files, student evaluations and other relevant teaching files).
Alumni records, including birthplaces, years of birth, dates of matriculation and conferrals of degrees. These records are available to former students after registering through Granchester's Alumni portal. Department for Education records, showing how certain demographic groups (such as first-generation students) could be expected, on average, to progress. These records do not contain names or identification numbers.
Under their security policy, the University encrypts all of its personal data records in transit and at rest.
フランクは、教育の質を向上させるため、工学部の学生の成績が教育省の期待値とどの程度一致しているかを調査したいと考えています。彼はアンナのデータ保護に関する研修コースを受講しており、目標達成に必要な範囲を超えて個人データを使用するべきではないことを理解しています。そこで、学生の過去の出身校、当初の成績、現在の成績、初めて進学した大学など、一部のデータのみをエクスポートするプログラムを作成しました。記録は個々の学生レベルで保管したいと考えています。アンナの研修を踏まえ、フランクは学生番号をアルゴリズムにかけ、異なる参照番号に変換します。各記録を継続的に更新できるよう、毎回同じアルゴリズムを使用します。
アンナの業務の一つは、GDPRの要件に従い、処理活動の記録を完了することです。GDPRの要件に従い、アンナからメールによるリマインダーを受け取った後、フランクはアンナにパフォーマンスデータベースについて連絡します。
アンはフランクに、個人データを最小限に抑えるだけでなく、大学は既存データの新たな利用が許容されるかどうかを確認する必要があると説明した。また、GDPRの下では、データ処理を実施する前にリスク分析を実施する必要があるのではないかとも考えている。アンナは追加調査を行った後、フランクとこの件についてさらに話し合う予定だ。

フランクは空き時間に分析作業を行いたいと考え、データを自宅のノートパソコン（暗号化されていない）に転送しました。ところが、大学にノートパソコンを持っていく途中、電車の中で紛失してしまいます。その日、フランクは互換性のある処理について話し合うため、アンナと面会する必要がありました。セキュリティインシデントを報告する必要があるため、同時にアンナにもノートパソコンの紛失について伝えることにしました。
アンナは、この状況ではリスク分析は必要ないと考えるでしょうか?
A. データ対象者はフランクの現在の生徒ではない
B. 処理はデータ主体の権利に悪影響を及ぼさない
C. フランクが処理に使用しているアルゴリズムは技術的に健全である
D. データ主体は、当初の処理に対して明確な同意を与えた
Answer: (解答を表示する**)**
リスク分析とは、組織の個人データ処理活動に影響を及ぼす可能性のある潜在的な脅威と脆弱性を特定、評価、軽減するプロセスです。リスク分析は一度限りの活動ではなく、継続的な監視と更新を必要とする動的なプロセスです。また、リスク分析はGDPRへのコンプライアンスの代替手段ではなく、法的義務とベストプラクティスを特定し、対処することでコンプライアンスを確保するためのツールです。
GDPRによると、組織は、データ主体の権利と自由に高いリスクをもたらす可能性のある、新規または大幅に増加する処理活動を開始する前に、データ保護影響評価（DPIA）を実施する必要があります。DPIAは、そのような処理活動に関連するリスクを特定、評価、軽減することを目的とした、体系的かつ文書化されたプロセスです。DPIAは、管理者（処理の目的と手段を決定する個人または団体）またはその代理人、あるいはその代理人によって実施されなければなりません。
このシナリオでは、フランクは、教育省の期待値に基づき、生徒の成績データを分析するという新たな処理活動について、DPIAを実施しています。この処理活動は、生徒の明示的な同意や認識なしに個人データを収集、保管、使用、転送することを伴うため、生徒の権利と自由にとって大きなリスクとなります。したがって、フランクはこの処理活動を開始する前に、DPIAを実施する必要があります。
ただし、この要件にはいくつかの例外があります。その一つは、処理活動に個人データが含まれ、その個人データが当初の収集目的またはその他の処理目的とはもはや関連がない場合です。この場合、フランクは、既存の個人データが新たな目的に適切かつ関連性があり、必要な範囲に限定されていることを保証できる限り、DPIAを実施することなく既存の個人データを使用することができます。
したがって、この状況では、データ主体がフランクの現在の生徒ではなくなった限り、アンナはリスク分析は不要であると判断するでしょう。つまり、フランクは、既存の生徒記録が適切かつ関連性があり、新しい目的に必要なものに限定されていることを保証できる限り、DPIAを実施することなく既存の生徒記録を使用することができます。
参照：
リスクとデータ保護影響評価（DPIA）| ICO
GDPR リスク評価とは何ですか? なぜ重要なのですか?
GDPRコンプライアンスリスク評価のベストプラクティス | Accountable
GDPRコンプライアンスにリスク評価が不可欠な理由

最新問題**: 36**
個人データ漏洩通知に関する事例に関するEDPBガイドライン01/2021によると、求人応募データ（オンライン申請フォームから送信され、ウェブサーバーに保存されているもの）の流出により、権限のない人が個人情報にアクセスできるようになったら、主にどのような種類の漏洩とみなされますか？
A. 整合性違反。

B. 精度違反です。
C. 可用性違反。
D. 機密漏洩。
Answer: D (メーッセージを残す**)**
EDPBの 個人データ漏洩通知に関する事例」ガイドライン01/2021によると、機密性漏洩は、個人データが不正な第三者に開示または利用可能になった場合に発生します。これは、ウェブサイトから求人応募データが流出し、ハッカーや競合他社などの不正な第三者が個人情報にアクセスできるようになる場合が該当します。この種の漏洩は、個人情報の盗難、詐欺、差別、または風評被害につながる可能性があるため、データ主体の権利と自由にとって大きなリスクとなる可能性があります。したがって、データ管理者は、データが暗号化または匿名化されている場合、または管理者がその後の措置を講じて高リスクが顕在化する可能性がなくなった場合を除き、遅滞なくデータ主体に通知する必要があります。

最新問題**: 37**
What is true if an employee makes an access request to his employer for any personal data held about him?
A. The employer can automatically decline the request if it contains personal data about a third person.
B. 情報が電子的にのみ保持されている場合、雇用主は要求を拒否できます。
C. 雇用主は従業員に関して保有するすべての情報を提供する必要があります。
D. 免除が適用されない限り、雇用主は従業員に関して保持されているすべての情報を提供する必要があります。
Answer: D (メーッセージを残す**)**
英国GDPRによると、従業員は雇用主から個人データのコピーやその他の補足情報にアクセスし、受け取る権利を有します。これはデータ主体アクセス要求（DSAR）と呼ばれます。雇用主は、要求が複雑または過度でない限り、要求を受領してから1ヶ月以内に、遅滞なくDSARに回答しなければなりません。雇用主は、要求された情報を合理的に検索し、アクセス可能で簡潔かつ理解しやすい形式で提供する必要があります。雇用主は、例外または制限が適用される場合、または要求が明らかに根拠がない、または過度である場合にのみ、情報提供を拒否できます。雇用関係において適用される可能性のある例外には、法的秘匿特権、経営予測、機密情報照会、交渉、規制機能、犯罪歴などがあります。雇用主は、情報を安全に開示し、従業員の権利とデータの出所を従業員に通知する必要があります。参考資料：
* アクセス権 | ICO
* 雇用主向けの個人情報アクセス要求に関するQ&A | ICO
* データ主体によるアクセス要求（雇用主向けガイド）| DavidsonMorris

最新問題**: 38**
シナリオ
次の質問に答えるには、以下を使用してください。
従業員数が急速に増加したため、A 社は給与計算業務を B 社にアウトソーシングすることを決定しました。B 社は、大規模な顧客基盤を持ち、業界で確固たる評判を誇る定評のある給与計算サービス プロバイダーです。
B社がA社向けに提供する給与計算ソリューションは、A社の各工場に設置された生体認証入退室システムから得られる勤怠データの収集に依存しています。B社は生体認証データを保有しませんが、関連データはB社の英国サーバーにアップロードされ、給与計算サービスの提供に使用されます。B社の本番システムには、A社の従業員一人ひとりに関する以下の情報が保存されます。
名前
住所
生年月日

給与番号
国民保険番号
病気休暇手当の受給資格
出産・育児手当の受給資格
休暇の権利
年金および給付金拠出金
労働組合の寄付
ジェニーは A 社のコンプライアンス担当者です。彼女はまず、A 社が新しい勤怠システムに関連してデータ保護影響評価を実施する必要があるかどうかを検討しましたが、それが必須かどうかはわかりません。
しかし、ジェニーはGDPRに基づき、B社に対し、勤怠データを給与計算サービスの提供目的にのみ使用し、データ保護のために適切な技術的および組織的なセキュリティ対策を講じることを義務付ける正式な書面による契約が必要であることを知っています。ジェニーはB社に対し、自社のデータ保護責任者（DPO）から助言を受けることを提案します。B社にはDPOはいませんが、契約締結のため、条項の全てに同意することに同意します。A社は契約を締結します。
数週間後、B社はA社との契約期間中に、給与計算サービスの機能強化を目的とした別のプロジェクトに着手し、C社に協力を依頼しました。C社は、B社の新しいデータベースを作成するために、B社の稼働中のシステムからすべての個人データを抽出することに同意しました。
このデータベースは、C社の米国サーバー上にホストされたテスト環境に保存されます。データはITテストの目的にのみ使用されるため、両社はサービス契約にデータ処理に関する条項を含めないことに合意しています。
残念ながら、C社の米国サーバーは時代遅れのITセキュリティシステムでしか保護されておらず、C社がプロジェクトに着手して間もなくサイバーセキュリティインシデントに見舞われました。その結果、A社の従業員に関するデータがC社のウェブサイトにアクセスするすべての人に公開されてしまいました。A社は、その後の調査に関連してジェニーが監督当局から書簡を受け取るまで、この事実を知りませんでした。ジェニーは侵害に気づき次第、影響を受ける全従業員に通知しました。
GDPRでは、企業が適切な技術的および組織的対策を実施できる能力を十分に保証することが求められています。B社がこの要件を満たす最も現実的な方法は何でしょうか？
A. 認定機関の勧告に沿った対策を実施している企業を採用します。
B. A 社の IT チームにアドバイスと技術サポートを依頼します。
C. 自社のサービスを改善するために他社のデータを利用することを避ける。
D. 適切な監督当局とともに企業の対策を審査する。
Answer: A (メーッセージを残す)
GDPR1234 の第 82 条は、GDPR の違反の結果として物質的または非物質的損害を被った人物に対する補償および責任の権利を規定しています。
第 821234 条の第 4 項では、管理者または処理者は、損害の原因となった事象についていかなる責任も負わないことを証明した場合、第 2 項 (GDPR に違反する処理によって生じた損害に対する責任を負わせる) に基づく責任を免除されると規定されています。したがって、GDPR に基づく賠償および責任の権利では、データ管理者 (またはデータ処理者) が損害を引き起こした事象に対していかなる責任も負わないことを証明した場合、責任が免除されます。
参照：
1: GDPR第82条 - 補償および責任の権利 - 一般データ保護規則（GDPR）
2 :GDPR第82条 - 補償および責任の権利 - GDPR.eu
3: GDPR第82条: 補償および責任の権利 - Advisera

4: GDPR第82条 | 補償および責任の権利

最新問題: **39**
ほとんどのプロセッサーがデータ処理活動に関連して保持しなければならない記録に含める必要がないのは次のどれですか?
A. プロセッサが代理を務める各コントローラの名前と連絡先の詳細。
B. プロセッサが機能している各コントローラに代わって実行される処理のカテゴリ。
C. プロセッサが行動している各コントローラに代わって実行される第三国への個人データの転送の詳細。
D. プロセッサが代理を務める各コントローラに代わってプロセッサが実行する処理活動に関連して実施されたデータ保護影響評価の詳細。
Answer: D (メーッセージを残す**)**
GDPR によれば、処理者は各管理者に代わって実行されるすべてのカテゴリーの処理活動の記録を保持しなければならず、これには以下の情報が含まれます12。
* 処理者（複数可）および処理者が代理を務める各管理者（該当する場合）の名前と連絡先、および管理者または処理者の代表者、およびデータ保護責任者の名前と連絡先。
* 各管理者に代わって実行される処理のカテゴリー
* 該当する場合、第三国または国際機関への個人データの移転（当該第三国または国際機関の特定を含む。また、第49条第1項第2段落に規定する移転の場合には、適切な保護措置の文書化を含む。）
* 可能な場合には、第32条第1項に規定する技術的及び組織的安全対策の概要。
記録は書面（電子形式を含む）で作成され、監督機関の要請に応じて開示されなければなりません。記録保持義務は、従業員数が250人未満の企業または組織には適用されません。ただし、当該企業または組織が行う処理がデータ主体の権利および自由に対するリスクをもたらす可能性が高い場合、処理が偶発的でない場合、または処理に特別なカテゴリーのデータまたは犯罪歴や違法行為に関連する個人データが含まれる場合は除きます。
GDPRは、処理者が各管理者に代わって行う処理活動に関して実施したデータ保護影響評価（DPIA）の詳細を、処理者に対し記載することを義務付けていません。DPIAは、プロジェクトのデータ保護リスクを特定し、最小限に抑えるためのプロセスです。特定の種類の処理が自然人の権利と自由に高いリスクをもたらす可能性がある場合、管理者はDPIAを実施する責任があります。処理者は管理者によるDPIAの実施を支援することはできますが、処理活動の記録にそれを文書化する必要はありません。
したがって正解はDです。参考文献：
* GDPR第30条(2)
* GDPR第35条
* ICO、ドキュメント1
* ICO、データ保護影響評価1

最新問題: **40**
ある住宅所有者が、玄関と玄関ホールを撮影する動体検知型監視システムを設置しました。カメラは公共エリアを撮影せず、住宅所有者の所有地のみを撮影します。システムは住宅所有者の居住地の法律に基づき当局に申告済みであり、敷地内に入る際には、そのエリアがビデオ監視対象であることを示す標識が目に入ります。なぜ住宅所有者は、監視カメラシステムによって記録された映像の処理に関して、世帯免除を適用できないのでしょうか？
A. GDPRは監視カメラ画像を家庭内例外から明確に除外している
B. 監視カメラシステムは、撮影範囲に入ってきた人物を撮影する可能性があります。

C. 監視カメラシステムは、住宅所有者の家族の生体情報を取得する可能性があり、これは特別なカテゴリの個人データの処理とみなされます。
D. 家主は監視カメラシステムの一部としてどのようなセキュリティ対策が実施されているかを指定していない
Answer: B (メーッセージを残す**)**

最新問題**: 41**
2016 年のガイダンスでは、英国の情報コミッショナー事務局 (ICO) は、データ主体に何を提供するために 階層化された通知」を使用することの重要性を再確認しましたか?
A. 簡単な情報が記載されたプライバシー通知で、詳細情報へのアクセスも提供します。
B. ウェブサイトで Cookie の使用をオプトアウトした場合の結果を説明するプライバシー通知。
C. 個人データを第三者に転送する際に適用されるセキュリティ対策の説明。
D. 書面による同意が求められる加盟国において、書面による同意を提供するための効率的な手段。
Answer: (解答を表示する**)**
説明

最新問題**: 42**
シナリオ
次の質問に答えるには、以下を使用してください。
ブレイディ氏はニュージーランドを拠点とするコンピュータプログラマーで、2年間にわたり自身のビジネスを経営しています。ブレイディ氏のビジネスは、欧州経済領域（EEA）全域の顧客に低価格のサービススイートを提供しています。これらのサービスは、新規および意欲的な中小企業経営者をターゲットにしています。ブレイディ氏の会社 Brady Box」は、ウェブページのデザインサービス、ソーシャルネットワーキングサービス SNS)、そしてオンラインストアの運営を支援するコンサルティングサービスを提供しています。
残念ながら、ブレイディ氏は苦情を受けています。アンナという名の顧客が最近、新製品の企画書をブレイディボックスのチャットエリア（公開されている)にアップロードしました。2週間後に間違いに気づき、その文書を削除したものの、アンナ氏はウェブサイトを定期的に監視していたにもかかわらず、この誤りに気付かなかったとしてブレイディボックスの責任を問うています。ブレイディ氏は、自分が責任を負うべきではないと考えています。
もう一人の顧客、フェリペは、自分の個人情報がHermes Designsというサードパーティの請負業者に転送されたことを知って驚き、自分のビジネス計画に関する機密情報が悪用されるのではないかと心配しています。ブレイディは、欧州のプライバシー規則に違反したとは思っていません。彼は、要求されたサービスの履行において個人データが特定のサードパーティに転送される可能性があることを明示的に記載したプライバシー通知をすべての顧客に提供しています。フェリペはプライバシー通知を読んだが、長くて複雑だったと言います。ブレイディは、Hermes Designsの誠実さを個人的に保証できるため、フェリペが心配する必要はないと主張し続けています。実際、Hermes Designsは、フェリペのような顧客のために、カスタマイズされたバナー広告のサンプルを作成することを率先して行っています。ブレイディは、現在Hermes DesignsのWebページに掲載されているサンプルバナー広告へのリンクを喜んで提供します。Hermes Designsは、これらの顧客へのダイレクトマーケティングをフォローアップする予定です。
ブレイディ氏は、別の顧客であるセルジュ氏から、自身の発言がブレイディボックスのホームページ上のグラフィックコラージュに使用されていることに憤慨していると伝えられ、驚きました。この発言はセルジュ氏の名前で表記されています。しかし、ブレイディ氏は訴訟を懸念していませんでした。セルジュ氏に返信し、この発言はブレイディボックスのソーシャルネットワーキングサー

ビス（SNS）で見つけたと伝えました。セルジュ氏自身がこの発言を投稿したからです。返信の中で、ブレイディ氏は礼儀として発言を削除することを申し出ました。
顧客からの苦情はあるものの、ブレイディ氏のビジネスは好調だ。彼は、明確な役割分担を定めたサードパーティの広告ネットワークを通じたオンライン行動ターゲティング広告（OBA）で収入を補っている。一部の顧客はOBAの存在をはっきりと認識していないものの、広告には役立つ商品やサービスが掲載されていることに、ブレイディ氏は満足している。
欧州のプライバシー慣行の現在の傾向に基づくと、Brady Box が欧州に進出した場合、同社のオンライン行動ターゲティング広告 (OBA) のどの側面が不十分になる可能性が高いでしょうか。
A. サードパーティの広告ネットワークとの契約。
B. 広告の内容が承認される必要がある。
セクション: (なし)
説明
C. ウェブサイト内のセキュリティのレベル。
D. オプトインのオプションがない。
Answer: D (メーッセージを残す**)**

最新問題**: 43**
次の手順をお読みください。
* どの従業員がどのデバイスやアプリからクラウドサービスにアクセスしているかを把握
* アプリやデバイスのデータをロックダウンする
* アプリとデバイスのコンプライアンスを監視および分析する
* アプリケーションのライフサイクルを管理する
* データ共有を監視する
組織は次のどれを実行するためにこれらの手順を実行する必要がありますか?
A. GDPR に準拠した Privacy by Design プロセスを追求します。
B. GDPR に準拠した従業員監視プロセスを導入します。
C. 安全な Bring Your Own Device (BYOD) プログラムを維持します。
D. クラウドベンダーが社内データ使用ポリシーに準拠していることを確認します。
Answer: C (メーッセージを残す**)**
説明/参考資料: https://www.itproportal.com/features/heading-off-the-spectre-of-gdpr-compliance-with-secure-byod/

最新問題**: 44**
OECDガイドラインの重要な要素の一つは「個人参加原則」です。一般データ保護規則（GDPR）のどの部分がこの原則に最も近いのでしょうか？
A. 第13条および第14条に規定されている情報要件
B. 第6条から第9条に規定される適法な処理基準
C. 第33条および第34条に規定されている違反通知要件
D. 第12条から第22条に基づいてデータ主体に付与される権利
Answer: D (メーッセージを残す**)**

最新問題**: 45**

2016 年のガイダンスでは、英国の情報コミッショナー事務局 (ICO) は、データ主体に何を提供するために 階層化された通知」を使用することの重要性を再確認しましたか?
A. 書面による同意が求められる加盟国において、書面による同意を提供するための効率的な手段。
B. 個人データを第三者に転送する際に使用されるセキュリティ対策の 1 つ。
C. ウェブサイトで Cookie の使用をオプトアウトした場合の結果を説明するプライバシー通知。
D. 簡単な情報が記載されたプライバシー通知で、詳細情報へのアクセスも提供します。
Answer: D (メーッセージを残す**)**

最新問題**: 46**
多国籍企業が、ヨーロッパに拠点を置く従業員を含むすべての現従業員および潜在的な従業員に対して身元調査を実施したい場合、その企業はどのような重要な規定に従う必要がありますか?
A. 身元調査は、ヨーロッパに拠点を置く従業員を含むすべての従業員からの事前の通知と明示的な同意がある場合にのみ許可されます。
B. ヨーロッパの従業員に対する身元調査は許可されない可能性がありますが、企業は正当な利益に基づいてリストを作成し、雇用に不適格な個人を特定することができます。
C. 欧州の従業員に対する身元調査は、データ保護法と雇用法に基づいて行われますが、加盟国によって異なる場合があります。
D. 従業員の身元調査は、すべての従業員に事前に通知した場合にのみ実行できます。
Answer: (解答を表示する**)**

最新問題**: 47**
次の質問に答えるには、以下を使用してください。
ProStorageは、オランダに本社を置く多国籍クラウドストレージプロバイダーです。CEOのルース ･ブラウン氏は、成長のために2本柱の戦略を立てました。1) ProStorageの顧客ベースを世界中に拡大し、2) 効果的なチームを効率的に採用してProStorageの営業部隊を増強することです。この戦略の実行は、ルースの健康状態により、最近、労働時間が制限され、潜在顧客に会うために出張することも困難になったため、複雑になっています。ProStorageの人事部とルースの首席スタッフは現在協力して、彼女のスケジュールを管理し、彼女がすべての医療予約を確実に受けられるようにしています。後者は、ルースが前回インドを旅行した際に健康上の緊急事態に見舞われ、ニューデリーで入院して以来、特に重要になっています。ルースの家族と連絡が取れなかったため、病院はProStorageに連絡し、首席スタッフと連絡を取ることができました。首席スタッフは、人事部長のメアリーと連携していました。
ルースが ProStorage を開始したときのリクエストに応じて、医師に情報を提供しました。ジャッキーは InstaHR を使用するためにどのような転送メカニズムを推奨すべきでしょうか?
A. 従業員の明示的な同意。
B. 拘束力のある企業規則。
C. 標準契約条項

D. 適切性
Answer: A (メーッセージを残す**)**

最新問題**: 48**
シナリオの要約:
WeScanYou は、EU、英国、インド、オーストラリアの病院で使用されている診断ツール (Scan4You) を提供しています。
データはアイルランドのサーバーで処理されます。
* 中央行政 :ドイツ
* IT開発 :オーストラリア
* データ戦略 :インド
* EU実装とGDPRコンプライアンス :フランス
ソフトウェア エンジニアによる妨害行為の後、画像データと自動診断 (名前や連絡先の詳細は不明) が公開されました。
質問 :
主要事業所の概念に関する EDPB 意見 04/2024 に基づくと、潜在的なデータ侵害はどの国に報告する必要がありますか?
A. ドイツ。中央行政の所在地だからです。
B. アイルランド。データ処理が行われる場所だからです。
C. GDPR の実装とコンプライアンスが処理される場所であるフランス。
D. EU 内に主要な施設がないため、患者が居住する各 EU 加盟国。
Answer: C (メーッセージを残す**)**
GDPRでは、処理の目的と手段に関する決定が別のEU施設で行われ、その施設がそれらの決定を実施する権限を有する場合を除き、EU内の管理者の「主要施設」をEU内での中央管理の場所として定めています（GDPR第4条（16））。
EDPB意見04/2024では以下が明確にされています。
* GDPR コンプライアンスの意思決定と実装が他の場所で行われる場合、主要な施設は自動的に中央管理部門 (HQ) になるわけではありません。
* むしろ、処理の目的と手段に関する決定が効果的に行われ、実行される場所です。
* EU 内にそのような機関が存在しない場合は、各加盟国の監督当局が権限を持つことになります (違反通知が複数回行われることを意味します)。
#このシナリオでは:
* ドイツは本部ですが、中央行政だけでは EU の処理に関する決定は行われません。
* アイルランドはサーバーをホストしていますが、目的を決定したり、GDPR の遵守を確保したりすることはありません。
* フランスには、EU における GDPR の実装とコンプライアンスの責任が明確に与えられています。
したがって、フランスは、GDPR 第 56 条および EDPB ガイダンスに基づく「主要事業所」として適格となります。
つまり、データ侵害はすべての加盟国ではなく、フランスの監督機関 (CNIL) に報告する必要があるということです。
#参照 :
* GDPR第4条(16)（主要事業所の定義）。
* GDPR、第56条（ワンストップショップメカニズム）。
* 主要事業所の概念に関する EDPB 意見 04/2024 (管理者は、GDPR コンプライアンス決定が実施される監督機関に報告する必要があります)。
* CIPP/E 教科書（第3 版）、第 13 章「監督と執行」（主要事業所および主導監督機関）。

最新問題: **49**
ある小学校が、生徒の出席状況を追跡するために顔認識技術を利用する予定です。この処理の法的根拠となり得るのは次のどれですか？
A. 学校は各カメラの近くに注意書きを設置します。
B. 学校は生徒から明示的な同意を得ます。
C. 処理は学校が追求する正当な利益のために必要です。
D. 州法により、出席確認には顔認識が義務付けられています。
Answer: B (メーッセージを残す**)**
参考 :https://www.jdsupra.com/legalnews/let-s-face-it-facial-recognition-1134180/

最新問題: **50**
GDPR第32条は、管理者と処理者の両方に適用される3つのセキュリティ領域を規定しています。これらには、以下のすべてが含まれますが、次のどれが該当しますか？
A. 同意の管理と撤回。
B. インシデントの検出と対応。
C. 予防的なセキュリティ。
D. 救済セキュリティ。
Answer: A (メーッセージを残す**)**
A. 同意の管理と撤回。GDPR第32条は、管理者と処理者に対し、処理のリスクに応じたセキュリティレベルを確保するための適切な技術的および組織的措置を実施することを義務付けています。これらの措置は、最新の技術水準、実施費用、処理の性質、範囲、状況および目的、そして自然人の権利と自由に対する様々な発生可能性と重大性のリスクを考慮する必要があります。第32条が対象とするセキュリティの3つの領域は以下のとおりです。
予防的セキュリティ :これは、個人データへの不正アクセス、開示、改ざん、紛失、破壊といったセキュリティインシデントの発生を防止または低減することを目的とした対策を指します。予防的セキュリティ対策の例としては、暗号化、仮名化、アクセス制御、ファイアウォール、ウイルス対策ソフトウェアなどが挙げられます。
インシデント検知 -対応 :セキュリティインシデントを検知、分析、封じ込め、根絶、復旧し、関係当局およびデータ主体に通知し、事実と対応内容を文書化することを目的とした対策を指します。インシデント検知 -対応策の例としては、セキュリティ監視、ログ記録、監査、インシデント対応計画、侵害通知手順などが挙げられます。
救済的セキュリティ :これは、物理的または技術的なインシデントが発生した場合に、個人データの可用性とアクセスを適時に回復し、セキュリティインシデントがデータ主体に及ぼす悪影響を軽減することを目的とした措置を指します。救済的セキュリティ対策の例としては、バックアップ、災害復旧、事業継続、補償などが挙げられます。
同意の管理と撤回は、GDPR第32条で規定されているセキュリティの領域ではなく、GDPR第6条(1)(a)項および第7条に基づく同意に基づく処理の合法性に関する要件です。同意の管理と撤回には、特定の処理目的についてデータ主体から同意を取得、記録、更新、撤回するとともに、データ主体がいつでも同意を撤回できる権利があることを通知することが含まれます。参考：無料CIPP/E学習ガイド、35ページ、CIPP/E認定資格、17ページ、GDPR第32条、第6条(1)(a)項、第7条。

最新問題: **51**

欧州データ保護委員会 (EDPB) は、転送ツールが欧州連合 (EU) レベルに準拠した個人データ保護レベルを効果的に提供しているかどうかの再評価をいつ推奨しますか?
A. 個人データ漏洩後。
B. 3年ごと。
C. 継続的に。
D. 毎年です。
Answer: C (メーッセージを残す)
参考: https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf 個人データのEU保護レベルへの準拠を確保するための移転ツールを補完する措置に関するEDPB勧告01/2020によると、第三国に個人データを輸出する者は、移転する個人データの保護レベルに影響を及ぼす可能性のある第三国における動向を継続的に監視する必要があります1。つまり、輸出者は、標準契約条項、拘束的企業準則、行動規範、認証メカニズムなど、依存する移転ツールが、EUレベルに準拠した個人データ保護レベルを効果的に提供しているかどうかを再評価する必要があります。EDPBは、輸出者がこの再評価と、その結果生じる変更を文書化することを推奨しています1。
EDPB は、この再評価の期間を固定して指定しておらず、各移管の具体的な状況や第三国における関連する動向を考慮しながら、継続的に行う必要があると述べています。
参考文献:
1 :EUの個人データ保護レベルへの準拠を確保するための転送ツールを補完する措置に関するEDPB勧告01/2020、バージョン2.0、2021年6月18日に採択、パラグラフ85〜86。

最新問題: **52**
Under what circumstances might the "soft opt-in" rule apply in relation to direct marketing?
A. When an individual has not consented to the marketing.
B. When an individual's details are obtained from their inquiries about buying a product.
C. Where an individual's details have been obtained from a bought-in marketing list.
D. Where an individual is given the ability to unsubscribe from marketing emails sent to him.
Answer: B (メーッセージを残す)
The "soft opt-in" rule is an exception to the general requirement of obtaining consent before sending electronic mail marketing to individuals. It applies when the following conditions are met12:
* the sender has obtained the contact details of the recipient in the context of the sale or negotiations for the sale of a product or service to that recipient;
* the sender only sends direct marketing relating to its own similar products or services; and
* 受信者には、詳細が最初に収集されたときと、その後のすべてのメッセージの両方で、マーケティングを拒否またはオプトアウトする簡単な機会が与えられています。
オプションBは、個人が送信者から製品を購入することに関心を示しており、送信者が個人の詳細を使用して類似製品に関するマーケティング情報を送信できることを示唆しているため、これらの条件に該当します。ただし、個人が簡単にオプトアウトできる場合に限ります。その他のオプションは、「ソフトオプトイン」ルールの対象外です。これは、同意、事前の関係、またはオプトアウトの仕組みがないためです。参考：電子メールマーケティング | ICO、GDPRにおけるダイレクトマーケティングのルールと例外

最新問題: **53**

第 17 条および検索エンジンの場合の RTBF 基準に関する EDPB ガイドライン S'2019 に従うと、次のすべてがデータ主体のリストからの削除要求の有効な根拠となりますが、次の例外はありません。
A. 個人情報は、子供への情報社会サービス (ISS) の提供に関連して収集されました。
B. データ主体が同意を撤回し、処理の他の法的根拠はありません。
C. 個人データは検索エンジンプロバイダの処理には不要になった
D. 表現の自由と情報の自由の権利を行使するために必要な処理
Answer: D (メーッセージを残す)
GDPR 第 17 条によれば、データ主体は管理者から自己に関する個人データの消去を遅滞なく取得する権利を有し、管理者は、以下のいずれかの理由が当てはまる場合、遅滞なく個人データを消去する義務を負います: (a) 個人データが、収集またはその他の方法で処理された目的に関連して不要になった場合、(b) データ主体が処理の根拠となる同意を撤回し、処理の他の法的根拠がない場合、データ主体が第 21 条 (1) に従って処理に異議を唱え、処理の優先する正当な根拠がない場合、またはデータ主体が第 21 条 (2) に従って処理に異議を唱えた場合、(d) 個人データが違法に処理された場合、(e) 管理者が従う EU 法または加盟国の法律の義務を遵守するために個人データを消去する必要がある場合、(f) 個人データが第 8 条 (1) に言及する情報社会サービスの提供に関連して収集された場合。
しかし、第17条第3項は、表現の自由および情報の自由の権利を行使するために必要な範囲においては、消去権は適用されないと規定しています。したがって、これはデータ主体によるリストからの削除要請の正当な根拠とはなりません。参考文献：
GDPR第17条
GDPRに基づく検索エンジンにおける忘れられる権利の基準に関するEDPBガイドライン5/2019（パート1）

最新問題: **54**
次の状況のうち、個人が処理に対する同意を撤回できる可能性が最も高いのはどれですか?
A. 組織からマーケティング資料を受け取ることを希望しなくなったとき。
B. 最近転職して、同じ会社で働いていなくなったとき。
C. 医師が記録に残した診断結果に彼女が同意できないとき。
D. 彼女が現在の銀行を辞めて、別の銀行に移るとき。
Answer: A (メーッセージを残す)

最新問題: **55**
シナリオ
次の質問に答えるには、以下を使用してください。
アンナとフランクは二人ともグランチェスター大学で働いています。アンナはデータ保護を担当する弁護士で、フランクは工学部の講師です。大学では様々な種類の記録を保管しています。
* 学生記録には、氏名、学生番号、自宅住所、大学入学前の情報、大学の出席および成績記録、特別な教育ニーズの詳細、財務情報が含まれます。
* 自伝的資料（カリキュラム、専門家の連絡先ファイル、学生の評価、その他の関連する教育ファイルなど）を含むスタッフの記録。
* 卒業生の記録（出身地、生年、入学日、学位授与日など）。
これらの記録は、グランチェスターの卒業生ポータルに登録した卒業生が閲覧できます。
* 教育省の記録。特定の人口統計グループ（第一世代の生徒など）の平均的な進級見込みを示しています。これらの記録には、氏名や身分証明書番号は含まれていません。

* 大学はセキュリティ ポリシーに従い、転送中および保存中のすべての個人データ記録を暗号化します。
フランクは、教育の質を向上させるため、工学部の学生の成績が教育省の期待値とどの程度一致しているかを調査したいと考えています。彼はアンナのデータ保護研修コースを受講しており、目標達成に必要な範囲を超えて個人データを使用するべきではないことを理解しています。そこで、学生の過去出身校、当初の成績、現在の成績、初めて進学した大学など、一部のデータのみをエクスポートするプログラムを作成しました。記録は個々の学生レベルで保存したいと考えています。
フランクはアンナの訓練を踏まえ、生徒番号をアルゴリズムにかけ、異なる参照番号に変換します。彼は毎回同じアルゴリズムを使用することで、時間の経過とともに各記録を更新していきます。
アンナの業務の一つは、GDPRの要件に従い、処理活動の記録を完了することです。GDPRの要件に従い、アンナからメールによるリマインダーを受け取った後、フランクはアンナにパフォーマンスデータベースについて連絡します。
アンはフランクに、個人データを最小限に抑えるだけでなく、大学は既存データの新たな利用が許容されるかどうかを確認する必要があると説明した。また、GDPRの下では、データ処理を実施する前にリスク分析を実施する必要があるのではないかとも考えている。アンナは追加調査を行った後、フランクとこの件についてさらに話し合う予定だ。
フランクは空き時間に分析作業を行いたいと考え、データを自宅のノートパソコン（暗号化されていない）に転送しました。ところが、大学にノートパソコンを持っていく途中、電車の中で紛失してしまいます。その日、フランクは互換性のある処理について話し合うため、アンナと面会する必要がありました。セキュリティインシデントを報告する必要があるため、同時にアンナにもノートパソコンの紛失について伝えることにしました。
アンナは、この状況ではリスク分析は必要ないと考えるでしょうか?
A. データ対象者はフランクの現在の生徒ではない
B. 処理はデータ主体の権利に悪影響を及ぼさない
C. データ主体は、当初の処理に対して明確な同意を与えた
D. フランクが処理に使用しているアルゴリズムは技術的に健全である
Answer: C (メーッセージを残す**)**

最新問題**: 56**
EUにおけるデータ保持は、データ保持指令（2006/24/EC）によって確立された法的枠組みによって支えられてきました。なぜこの指令はEU法の一部ではなくなったのでしょうか？
A. この指令は、プライバシーと電子通信に関する EU 指令に置き換えられました。
B. この指令は、一般データ保護規則に置き換えられました。
C. この指令は欧州司法裁判所によって無効とされました。
D. この指令は欧州人権裁判所によって無効とされました。
Answer: C (メーッセージを残す**)**
データ保持指令（2006/24/EC）は、加盟国に対し、公的に利用可能な電子通信サービスまたは公衆通信ネットワークのプロバイダーが、重大犯罪の防止、捜査、摘発および訴追を目的として、特定のデータを6か月から2年間保持することを保証することを義務付ける法的枠組みでした1。しかし、2014年4月8日、欧州連合司法裁判所（CJEU）は、この指令が、管轄権のある国内当局による保持データへのアクセスを厳密に必要な範囲に制限することなく、私生活の尊重と個人データの保護に関する基本的権利に対する広範かつ特に深刻な干渉を伴うとして、無効であると宣言しました2。CJEUはまた、この指令が、データの乱用リスクおよびデータへの不法なアクセスと使用に対するデータの効果的な保護を確保するための十分な安全策を提供していないと判断しました2。したがって、この指令はもはやEU法の一部ではありません。
参照：

欧州議会および理事会の指令2006/24/EC
欧州連合司法裁判所 プレスリリース No.54/14
GDPRとデータ保持についてご理解を深めていただければ幸いです。他にご質問がございましたら、お気軽にお問い合わせください。

最新問題: **57**
Please use the following to answer the next question:
WonderkKids provides an online booking service for childcare. Wonderkids is based in France, but hosts its website through a company in Switzerland. As part of their service, WonderKids will pass all personal data provided to them to the childcare provider booked through their system. The type of personal data collected on the website includes the name of the person booking the childcare, address and contact details, as well as information about the children to be cared for including name, age, gender and health information. The privacy statement on Wonderkids' website states the following:
"WonderkKids provides the information you disclose to us through this website to your childcare provider for scheduling and health and safety reasons. We may also use your and your child's personal information for our own legitimate business purposes and we employ a third-party website hosting company located in Switzerland to store the data. Any data stored on equipment located in Switzerland meets the European Commission provisions for guaranteeing adequate safeguards for you and your child's personal information.
We will only share you and your child's personal information with businesses that we see as adding real value to you. By providing us with any personal data, you consent to its transfer to affiliated businesses and to send you promotional offers."
"We may retain you and your child's personal information for no more than 28 days, at which point the data will be depersonalized, unless your personal information is being used for a legitimate business purpose beyond 28 days where it may be retained for up to 2 years."
"We are processing you and your child's personal information with your consent. If you choose not to provide certain information to us, you may not be able to use our services. You have the right to: request access to you and your child's personal information; rectify or erase you or your child's personal information; the right to correction or erasure of you and/or your child's personal information; object to any processing of you and your child's personal information. You also have the right to complain to the supervisory authority about our data processing activities." What direct marketing information can WonderKids send by email without prior consent of the person booking the childcare?
A. No marketing information at all.
B. Any marketing information at all.
C. Marketing information related to other business operations of WonderKids.
D. Marketing information for products or services similar to those purchased fromWonderKids.
Answer: D (メーッセージを残す)
According to the ePrivacy Directive, which regulates direct electronic marketing in the EU, consent is generally required before sending marketing emails or texts. However, there is an exception known as the
'soft opt-in', which allows marketing emails or texts to be sent on an opt-out basis if the recipient's details were collected "in the context of the sale of a product or a service" and the marketing is for "similar products or services" provided by the same organisation12. Therefore, WonderKids can send direct marketing information by email without prior consent of the person booking the childcare, as long as the information is about similar products or services to those purchased from WonderKids, and the person is given a clear and easy way to opt out of receiving such emails. The other options are not allowed under the ePrivacy Directive, unless the person has given explicit consent to receive them. References:

* Free CIPP/E Study Guide, page 33, section 4.1.3
* CIPP/E Certification, page 28, section 4.1.3
* Cipp-e Study guides, Class notes & Summaries, page 39, section 4.1.3
* Direct marketing rules and exceptions under the GDPR, paragraph 5
* Marketing | ICO, section "What does the 'soft opt-in' mean?"

最新問題**: 58**
法執行目的での通信トラフィック データの保持は、欧州データ保護法ではどのように扱われていますか?
A. ePrivacy 指令では、個々の EU 加盟国がこのようなデータ保持を行うことが許可されています。
B. ePrivacy 指令は、このようなデータ保持に関する EU 加盟国の規則を調和させます。
C. データ保持指令の廃止により、このようなデータ保持が許可されるようになりました。
D. GDPR では、このようなデータの保持は、犯罪の防止、捜査、検出、または訴追の目的でのみ許可されています。
Answer: B (メーッセージを残す**)**
eプライバシー指令は、電子通信の機密性を保護し、無差別な傍受や監視を防止することを目的とした欧州連合（EU）の指令です。2002年に採択され、2009年に改正されました。インターネットサービスプロバイダー、モバイルネットワーク事業者、オンラインプラットフォームなど、すべての電子通信サービス提供者に適用されます12。
eプライバシー指令の主な目的の一つは、法執行目的での通信トラフィックデータの保持が厳格な条件と保護措置の対象となるようにすることです。通信トラフィックデータとは、IPアドレス、タイムスタンプ、メタデータなど、電子通信の送信またはルーティングに関連するあらゆる情報を指します3。これらのデータは、管轄権を持つ各国当局が犯罪の防止、捜査、摘発、訴追、および国家安全保障の確保のために利用される可能性があります4。
しかし、eプライバシー指令は、EU加盟国が規則を統一することなく、このようなデータ保持を行うことを許可していません。指令第6条(1)(b)は、「加盟国は、トラフィックデータの保持に関して自国が講じるあらゆる措置がこの指令に適合することを確保しなければならない」と規定しています。したがって、各EU加盟国は、指令で定められた要件と制限を遵守する国内法を制定する必要があります12。
データ保持指令（DRD）は、EU加盟国全体で法執行目的で通信トラフィックデータを保持するための共通枠組みを確立することを目指した、以前のEU指令でした。2006年に採択され、2010年に改正されました。しかし、2014年に欧州連合司法裁判所（CJEU）によって手続き上の理由で無効化されました。CJEUは、DRDの一部規定が、個人のプライバシーへの恣意的な干渉から個人を保護する基本権憲章（CFR）第8条第2項など、他のEU指令や原則と矛盾していると判断しました56。
GDPRは、個人データ処理に関する規定を通じてDRDの一部を国内法に組み込むEUの新しい規則です。しかし、法執行目的での通信トラフィックデータの保持という問題には直接的には対処していません。その代わりに、GDPRは、個人データ処理に伴うリスクに見合ったセキュリティレベルを確保するために、プロバイダーに適切な技術的および組織的措置を講じることを義務付けています。これらの措置には、暗号化、仮名化、アクセス制御、アカウンタビリティ7が含まれます。GDPRはまた、個人データへのアクセス、訂正、消去、ポータビリティ、異議申し立てなど、個人データに関する特定の権利を個人に付与しています7。
したがって、現行のEU法では、EU加盟国全体で法執行目的で通信トラフィックデータを保持するための単一の法的根拠は存在しません。各加盟国は、eプライバシー指令で定められた原則と制限を尊重する独自の国内法を制定する必要があります。
参考文献:
eプライバシー指令
eプライバシー規制
通信トラフィックデータとは何ですか?

通信トラフィックデータはどのように保存されますか?
データ保持指令
データ保持指令がCJEUによって無効化
一般データ保護規則
あなたの個人データに関する権利は何ですか?
参考 :https://www.law.kuleuven.be/citip/en/archive/copy_of_publications/440retention-of-traffic-data-dumortier-goemans2f90.pdf (9)

最新問題**: 59**
次のどれが労働組合協議会の役割ではないでしょうか?
A. 従業員データのデータ漏洩違反に対して雇用主に課される罰金を決定します。
B. 従業員に影響を与える雇用主の特定の決定を承認するか拒否するかを決定します。
C. 従業員の個人データを処理できるかどうかを決定します。
D. どのような変更が従業員の労働条件に影響するかを判断します。
Answer: A (メーッセージを残す**)**
労働組合委員会は、ドイツ、フランス、スペイン、イタリアなど一部のヨーロッパ諸国に存在する従業員代表機関です。労働組合委員会は、各国の法律や労働協約に応じて様々な役割と権限を有しますが、一般的には、使用者との関係において従業員の利益を保護し、促進することを目的としています。労働組合委員会の一般的な役割には、以下のものがあります。
* 転勤、解雇、人員削減、労働時間、健康と安全など、従業員に影響を与える雇用主の特定の決定を承認するか拒否するかを決定します。
* 共同決定の原則に基づいて、従業員の個人データを処理できるかどうかを決定します。つまり、従業員の監視、評価、または管理を含むすべてのデータ処理については、雇用主は労働組合の同意を得る必要があります。
* 賃金、福利厚生、研修、社会福祉施設など、従業員の労働条件にどのような変更が影響するかを判断します。
しかし、労働組合は、従業員データの漏洩違反に対して雇用主に課される罰金を決定する役割を担っていません。これは、調査権および是正権を通じてデータ保護法の適用を監督する独立した公的機関であるデータ保護当局の役割です。労働組合は、データ保護当局に協力したり、従業員に代わって苦情を申し立てたりすることはできますが、雇用主に制裁を科す権限はありません。参考文献：無料CIPP/E学習ガイド、27ページ ;CIPP/E認定資格、13ページ。

最新問題**: 60**
電子商取引指令 2000/31/EC によれば、GDPR によって確認されるインターネット ウェブサイトを通じてサービスを提供する企業の 「設立地」はどこですか?
A. ウェブサイトをサポートする技術が配置されている場所
B. ウェブサイトがアクセスされる場所
C. 処理に関する決定が行われる場所
D. 顧客のインターネットサービスプロバイダーの所在地
Answer: (解答を表示する**)**
説明/参考資料: https://www.ohiobar.org/member-tools-benefits/publications/Ohio-Lawyer/the-european-general- data-protection-regulation-gdpr/

最新問題**: 61**
GDPR の第 58 条では、欧州連合 (EU) 加盟国の監督当局の権限について次のどれが説明されていますか?

A. 行政命令によって新しい法律を制定する権限。
B. 調査目的でデータにアクセスする権利。
C. 加盟国内で選出された公務員の目標を遂行する裁量権。
D. コントローラーが法廷で有罪と判断された場合に罰則を選択する権限。
Answer: (解答を表示する**)**
GDPR第58条は、EU加盟国の監督当局の権限を列挙しています。これらの権限には、管理者および処理者からデータおよび情報にアクセスする権利、ならびにそれらの施設および設備にアクセスする権利を含む調査権限が含まれます。この権限により、監督当局はGDPRの監視および執行という任務を遂行することができます。その他の権限は、GDPR第58条に基づく監督当局の権限ではありません。参考 :GDPR第58条 - 権限、GDPR第58条 - 権限 - GDPR、GDPR第58条 - GDPRhub

最新問題**: 62**
シナリオ
次の質問に答えるには、以下を使用してください。
あなたは香港に拠点を置く玩具メーカーに採用されました。同社は幅広い種類の人形、アクションフィギュア、ぬいぐるみを販売しており、世界中の様々な小売店で販売されています。同社は香港以外にオフィスを持たず、実際には香港以外で従業員を雇用していませんが、複数の現地販売契約を締結しています。同社が製造する玩具は、ヨーロッパ、アメリカ、アジアのあらゆる人気玩具店で販売されています。同社の収益の大部分は海外販売によるものです。
同社は現在、子供たちと会話したり交流したりできるコネクテッドトイの新シリーズを発売したいと考えています。同社のCEOは、これらのおもちゃがもたらす可能性の拡大を理由に、次なる大ヒット作になると宣伝しています。人形は、数学の計算や天気など、様々なテーマについて子供たちの質問に答えることができます。各人形にはマイクとスピーカーが搭載されており、Bluetooth経由でスマートフォンやタブレットに接続できます。半径10メートル以内にあるあらゆるモバイルデバイスも、Bluetooth経由でおもちゃに接続できます。また、人形は（同じメーカーの）他の人形と連携して相互に作用し、より充実した遊び体験を提供します。
お子様がおもちゃに質問をすると、そのリクエストはクラウドに送信され、分析されます。クラウドサーバー上で回答が生成され、人形に返されます。回答は人形に内蔵されたスピーカーから聞こえるため、まるでおもちゃが実際にお子様の質問に答えているかのように聞こえます。おもちゃのパッケージには、この機能の仕組みに関する技術的な詳細は記載されておらず、インターネット接続が必要であることも記載されていません。この機能に必要なデータ処理は、南アフリカにあるデータセンターに委託されています。しかしながら、貴社は消費者向けのプライバシーポリシーを改訂し、この点について明示していません。
同社は同時に、ゲームプレイ中に獲得したキャラクターを操作できる新たなゲームシステムの導入も計画している。このシステムには、近距離無線通信（NFC）リーダーを搭載したポータルが同梱される。このデバイスがアクションフィギュアのRFIDタグを読み取り、画面上でフィギュアが動き出す。各キャラクターにはそれぞれ固有の特徴や能力があり、ゲーム目標を達成することで追加の能力を獲得することもできる。タグに保存される情報は、フィギュアの能力に関する情報のみ。ゲーム中にキャラクターを簡単に切り替えることができ、フィギュアを家の外に持ち出してもキャラクターの能力はそのまま維持される。
この会社が GDPR に準拠する義務があるのはなぜですか?

A. 当社は EU にオフィスを構えています。
B. 当社は EU 内で従業員を雇用しています。
C. 会社のデータセンターは EU 域外の国にあります。
D. 同社の製品は EU の顧客に直接販売されています。
Answer: D (メーッセージを残す)
あなたは香港に拠点を置く玩具メーカーに採用されました。同社は幅広い種類の人形、アクションフィギュア、ぬいぐるみを販売しており、世界中の様々な小売店で販売されています。同社は香港以外にオフィスを構えておらず、実際には香港以外で従業員を雇用していませんが、複数の現地販売契約を締結しています。同社が製造する玩具は、ヨーロッパ、アメリカ、アジアのあらゆる有名玩具店で販売されています。同社の収益の大部分は海外販売によるものです。
同社は現在、子供たちと会話したり交流したりできるコネクテッドトイの新シリーズを発売したいと考えています。同社のCEOは、これらのおもちゃがもたらす可能性の拡大を理由に、次なる大ヒット作になると宣伝しています。人形は、数学の計算や天気など、様々なテーマについて子供たちの質問に答えることができます。各人形にはマイクとスピーカーが搭載されており、Bluetooth経由でスマートフォンやタブレットに接続できます。半径10メートル以内にあるあらゆるモバイルデバイスも、Bluetooth経由でおもちゃに接続できます。また、人形は（同じメーカーの）他の人形と連携して相互に作用し、より充実した遊び体験を提供します。
お子様がおもちゃに質問をすると、そのリクエストはクラウドに送信され、分析されます。クラウドサーバー上で回答が生成され、人形に返されます。回答は人形に内蔵されたスピーカーから聞こえるため、まるでおもちゃが実際にお子様の質問に答えているかのように聞こえます。おもちゃのパッケージには、この機能の仕組みに関する技術的な詳細は記載されておらず、インターネット接続が必要であることも記載されていません。この機能に必要なデータ処理は、南アフリカにあるデータセンターに委託されています。しかしながら、貴社は消費者向けのプライバシーポリシーを改訂し、この点について明示していません。
同社は同時に、ゲームプレイ中に獲得したキャラクターを操作できる新たなゲームシステムの導入を計画している。このシステムには、近距離無線通信（NFC）リーダーを搭載したポータルが同梱される。このデバイスがアクションフィギュアのRFIDタグを読み取り、画面上でフィギュアが動き出す。各キャラクターにはそれぞれ固有の特徴や能力があり、ゲーム目標を達成することで追加の能力を獲得することもできる。タグに保存される情報は、フィギュアの能力に関する情報のみ。ゲーム中にキャラクターを簡単に切り替えることができ、フィギュアを自宅以外の場所に持ち出しても、キャラクターの能力はそのまま維持される。
この会社が GDPR に準拠する義務があるのはなぜですか?
A . この会社は EU 内にオフィスを構えている。B . この会社は EU 内で従業員を雇用している。C . この会社のデータセンターは EU 域外の国にある。D . この会社の製品は EU の顧客に直接販売されている。
検証済み回答: D 。同社の製品はEUの顧客に直接販売されています。
GDPR1の第6条(1)によれば、個人データは、商品やサービスを提供し、またはその他の方法で活動を行う組織により処理され、それに関連して個人データの処理が正当な利益に関連するとみなされる可能性がある。ここでいう正当な利益とは、自身の名において、またはその代理で、または自身の目的で実行されるタスクの遂行から生じる利益である。ここでいう正当な利益とは、自身の名において、またはその代理で、または自身の目的で実行されるタスクの遂行から生じる利益である。ここでいう正当な利益とは、自身の名において、またはその代理で、または自身の目的で実行されるタスクの遂行から生じる利益である。ここでいう正当な利益とは、自身の名において、またはその代理で、または自身の目的で実行されるタスクの遂行から生じる利益である。ここでいう正当な利益とは、自身の名において、またはその代理で、または自身の目的で実行されるタスクの遂行から生じる利益である。ここでいう正当な利益とは、本人の名義で、本人に代わって、または本人自身の目的のために遂行される業務の遂行から生じる利益をいう。ここでいう正当な利益とは、本人の名義で、本人に代わって、または本人自身の目的のために遂行される業務の遂行から生じる利益をいう。

最新問題: **63**
処理アクティビティがプロファイリングとみなされるかどうかを判断する際に関係しないものは次のうちどれですか?
A. 処理に個人データとみなされるデータが含まれる場合
B. 処理がサードパーティベンダーによって実行される場合
C. 処理がデータ主体の行動を予測するために使用される場合
D. データの処理が自動化された手段によって行われる場合
Answer: C (メーッセージを残す)

最新問題: **64**
GDPR の「ワンストップショップ」メカニズムに関して正確な記述は次のうちどれですか?
A. データ保護監督当局の直接的な執行（違反の発見など）にのみ適用され、裁判手続きの開始や関与には適用されません。
B. さまざまな国に設立された公的機関によって実行されるプロセスから生じるプライバシーの問題に対処する権限を主導監督機関に与えます。
C. これにより、EU 内の複数の主導監督機関が、組織の同じデータ処理活動に対する権限を担うことになる可能性があります。
D. 関係する監督当局（主たる監督当局以外）は、組織がそれぞれの当局の加盟国にいかなる種類の施設も持っていない場合でも、例外的なケースにおいて組織に対して行動を起こすことができます。
Answer: (解答を表示する)

最新問題: **65**
GDPR では「処理」をどのように定義していますか?
A. 個人データの収集および記録を伴う行為。
B. 個人データまたは個人データ セットに対して実行される任意の操作または操作のセット。
C. データが収集された目的に適合する個人データの使用または開示。
D. 個人データまたは個人データ セットに対して自動化された手段によって実行される操作または操作のセット。
Answer: A (メーッセージを残す)
説明/参照: https://gdpr-info.eu/issues/processing/

最新問題: **66**
GDPR によると、データ保護責任者 (DPO) の主なタスクは何ですか?
A. 処理アクティビティの記録を作成し、維持します。
B. 管理者または処理者に代わってプライバシー影響評価を実施します。
C. 他の地域または欧州のデータ保護規定の遵守を監視するため。
D. 個人データ侵害を管轄の監督当局に通知するための手順を作成します。
Answer: B (メーッセージを残す)
GDPR の第 35 条によれば、管理者は、自然人の権利と自由に高いリスクをもたらす可能性のある処理を行う前に、データ保護影響評価 (DPIA) を実施する必要があります。
DPIAは、個人データ処理が個人データ保護に及ぼす潜在的な影響を評価し、軽減するためのプロセスです。管理者は、DPIAを実施するにあたり、DPO（指定されている場合）の助言を求めなければなりません。
DPOは、管理者によるDPIAの実施とGDPR要件への準拠の確保を支援することができます。また、DPIAの実施状況を監視したり、監督機関とデータ主体との連絡窓口として機能したりすることもできます。参考資料：

* GDPR第35条
* 欧州データ保護法と実務の教科書、第7章 「データ保護影響評価」、セクション7.2 「DPIAはいつ必要か？」、サブセクション7.2.1 「DPOの役割」
* データ保護責任者の役割と責任
参考: https://digitalguardian.com/blog/what-data-protection-officer-dpo-learn-about-new-role-required- gdpr-compliance

最新問題: **67**
ある企業は、欧州連合（EU）が適切なデータ保護レベルを備えているとみなしていない国に所在しています。標準契約条項に基づき、欧州経済領域（EEA）内の他の組織から個人データを輸入する場合、この企業には以下のどの義務がありますか？
A. 契約を自国の政府機関に提出します。
B. データ主体に通知し、同意を得ていることを確認します。
C. データ保護機関 (DPA) から要求された情報を 30 日以内に提供します。
D. 現地の法律が会社の契約上の義務の履行を妨げないことを確認します。
Answer: (解答を表示する**)**
GDPRでは、データ輸出者とデータ輸入者が適切な保護措置を講じている場合、十分なデータ保護水準を満たしていないEEA域外の国への個人データの移転が認められています1。こうした保護措置の一つとして、欧州委員会が採択した標準契約条項（SCC）があります。これは、移転がGDPRの要件に準拠することを保証する義務を両当事者に課すモデル条項です2。SCCには、データ主体の権利、データ保護当局の義務、当事者の責任および補償に関する条項も含まれています3。SCC に基づくデータ輸入者の義務の 1 つは、データ輸入者に適用される法律により、データ輸出者から受けた指示や契約上の義務を履行することが妨げられると考える理由がないこと、また、この法律が変更され、SCC で規定される保証や義務に重大な悪影響を及ぼす可能性がある場合は、その変更を認識し次第、速やかにデータ輸出者に通知することを保証することです。その場合、データ輸出者は、データの転送を一時停止し、契約を解除する権利を有します4。したがって、選択肢 D は、SCC に基づくデータ輸入者の義務、すなわち、現地の法律により契約上の義務を履行することが妨げられないようにするという義務を反映しているため、正解です。選択肢 A、B、C は不正解です。これらは、SCC に基づくデータ輸入者の義務ではありません。オプション A は、GDPR や SCC では必須ではありません。これは、データ輸入者が所在する国の法律で個人データの転送または開示前に契約書を自国の政府機関に提出することが義務付けられていない限り、データ輸入者は契約書を自国の政府機関に提出する必要がないためです5。オプション B はデータ輸入者の義務ではなく、データ輸出者の義務です。データ輸出者は、GDPR の第 13 条および第 14 条で義務付けられている情報をデータ主体に提供する必要があります。これには、データが第三国に転送されることや適切な保護措置が実施されていることなどが含まれます6。オプション C は SCC に固有のものではなく、GDPR に基づくすべての管理者または処理者の一般的な義務です。管理者または処理者は、監督機関と協力し、義務の遵守を証明するために必要なすべての情報を提供する必要があります7。参照: 1: GDPR 第46条(1) 2: 標準契約条項 (SCC) - 欧州委員会 3: EU 標準契約条項 (Word 文書) 4: 規則 (EU) 2016/679 に基づく第三国への個人データの移転に関する SCC 第5条(a) 5: 規則 (EU) 2016/679 に基づく第三国への個人データの移転に関する SCC 第5条(b) 6: 規則 (EU) 2016/679 に基づく第三国への個人データの移転に関する SCC 第9条 7: GDPR 第31条

最新問題: **68**
1973 年にデータ保護に関する国内法を最初に施行したのは次のどれですか?
A. フランス
B. スウェーデン
C. ドイツ

D. イギリス
Answer: (解答を表示する**)**
参照：
スウェーデンは1973年にデータ保護法と呼ばれる国家データ保護法を制定した最初の国でした。この法律は1974年7月1日に施行され、個人データを扱う情報システムにはスウェーデンデータ保護局のライセンス取得が義務付けられました。この法律は、コンピュータの利用と、政府やその他の機関による個人データの潜在的な悪用に対する国民の懸念を受けて制定されました。その後、この法律は1998年にEUデータ保護指令を施行する個人データ法に置き換えられました。参考文献 :データ法 (スウェーデン) - Wikipedia、データプライバシー法：現代データプライバシー法の簡潔な歴史 - eperi、スウェーデンプライバシー保護局 - Wikipedia
詳細はこちら
1en.wikipedia.org2blog.eperi.c

最新問題**: 69**
シナリオ
次の質問に答えるには、以下を使用してください。
Zandelay Fashion（以下「Zandelay」）は、アイルランドのダブリンに本社を置き、約650人の従業員を擁する、国際的なオンライン衣料品小売業者です。マーティンは最近任命されたデータ保護責任者であり、一般データ保護規則（GDPR）およびその他のプライバシー法の遵守を監督しています。
同社は、子供を含むあらゆる年齢層を対象に、男性用と女性用の衣料品ラインを提供しています。その過程で、顧客の嗜好やクレジットカード番号や銀行口座番号といった機密性の高い金融情報など、大量の顧客情報を処理しています。
収益成長を積極的に図るため、CEOのジェリーはマーティンに対し、顧客の購入履歴を分析し、プロファイリングに重点を置いた新しいモバイルアプリとロイヤルティプログラムを導入することを伝えた。マーティンはCEOに対し、(a) こうした活動に伴う潜在的なリスクを考慮すると、ザンデレイ社はこの新しい取り組みとプライバシーへの影響を評価するためにデータ保護影響評価を実施する必要があること、(b) この評価結果が、適切な保護措置を講じない場合に高いリスクが生じることを示している場合、ザンデレイ社はアプリとロイヤルティプログラムを導入する前に、アイルランドのデータ保護コミッショナーと事前協議を行う必要がある可能性があることを伝えた。
ジェリーはマーティンに対し、監督当局と直接交渉し、ザンデレイの事業計画と関連する処理活動の詳細を開示しなければならない可能性について不満を述べている。
Zandelay がデータ保護影響評価を実施する上で最も効果的に支援できるものは何でしょうか?
A. GDPR の第 38 条から第 40 条に記載されている DPIA に関する情報。
B. データ管理者が維持する必要があるデータ侵害の文書。
C. 地方監督当局によって発行された既存の DPIA ガイド。
D. データ管理者が維持する必要がある処理活動の記録。
Answer: C (メーッセージを残す**)**
データ保護影響評価（DPIA）は、個人データが関わるプロジェクトのデータ保護リスクを特定し、最小限に抑えるためのプロセスです。特に、個人に高いリスクをもたらす可能性のある新しい技術や処理を使用する場合に重要です1。英国GDPRでは、データ管理者は、そのような処理を開始する前にDPIAを実施し、DPIAで軽減できない高いリスクが示された場合は監督機関に相談することが義務付けられています1。英国GDPRは、DPIAの内容と方法に関する一般的なガイダンスも提供していますが、具体的な形式や手順は規定していません1。したがって、ZandelayのDPIA実施を効果的に支援するためには、英国のICOやアイルランドのDPC23などの現地監督機関が発行する既存のDPIAガイドを参照することが有用です23。これらのガイドは、DPIAの実施方法、DPIAに含めるべき内

容、リスクの評価と軽減方法、監督機関に相談するタイミングについて、より詳細で実践的なアドバイスを提供しています23。また、DPIAプロセスを説明するテンプレート、チェックリスト、事例、ケーススタディも提供しています23。これらのガイドに従うことで、ZandelayはDPIAが包括的で一貫性があり、英国GDPRおよび関連する国内法に準拠していることを保証できます。
他のオプションはオプション C ほど効果的ではありません。その理由は次のとおりです。
オプションA：英国GDPR第38条から第40条に記載されているDPIAに関する情報は、Zandelay社のDPIA実施を支援するにはあまりにも一般的かつ曖昧です。これらの条項は、DPIAの基本的な要件と原則を概説しているだけで、DPIAの実施方法、DPIAに含めるべき内容、リスクの評価と軽減方法に関する具体的なガイダンスは提供されていません1。Zandelay社がDPIAを効果的に実施するには、より詳細で実践的なアドバイスが必要です。
オプション B: データ管理者が保持する必要があるデータ侵害の文書は、DPIA の実施とは関係ありません。データ侵害とは、個人データの偶発的または違法な破壊、紛失、改ざん、不正開示、またはアクセスにつながるセキュリティ インシデントです1。データ管理者は、事実、影響、および講じた是正措置を含むすべてのデータ侵害を文書化し、監督機関および影響を受けた個人に遅滞なく通知する必要があります1。ただし、データ侵害は、個人データの処理の結果として個人に悪影響が生じる可能性のあるデータ保護リスクとは異なります2。DPIA は、プロジェクトのデータ保護リスクを特定して最小限に抑える事前予防策であり、データ侵害の結果に対処する事後対応的是正策ではありません2。
オプション D: データ管理者が保持する必要がある処理活動の記録は、Zandelay が DPIA を実施するのに十分ではありません。処理活動の記録とは、データ管理者またはデータ処理者による個人データの処理の目的、カテゴリ、受信者、転送、保持期間、セキュリティ対策に関する情報を含む文書です1。データ管理者は、その責任の下で処理活動の記録を保持し、監督機関の要求に応じてそれを提供する必要があります1。ただし、処理活動の記録は、データ保護リスクとその対処策をより詳細かつ体系的に分析する DPIA とは異なります2。処理活動の記録は、処理の性質、範囲、状況、目的など、DPIA に役立つ情報を提供する場合がありますが、処理の必要性、比例性、コンプライアンス、影響など、他の側面はカバーしていません2。
https://blog.netwrix.com/2021/02/17/データ保護影響評価/
https://ico.org.uk/for-organisations-2/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

最新問題**: 70**
第 29 条作業部会は、GDPR が ワォーラム ショッピング」を禁止していることを強調していますが、企業が何を行うと ワォーラム ショッピング」が発生しますか?
A. ビジネス上の懸念に最も共感してくれるデータ保護責任者を選択します。
B. 最も柔軟な慣行を持つ加盟国における主要事業所を指定します。
C. 侵害判決に対する控訴を複数の EU 機関に同時に提出します。
D. プライバシー保護の品質ではなくコストに基づいてサードパーティのプロセッサを選択します。
Answer: B (メーッセージを残す**)**
GDPRは、EU全体のデータ保護規則を調和させ、それらの規則の一貫性と有効性を確保することを目的としています。しかし、GDPRは、加盟国間の国内法、文化、慣行の違いにより、法律の解釈と適用に若干の差異が生じる可能性があることも認識しています。そのため、GDPRは管理者または処理者の 庄たる事業所」という概念を導入しています。これは、EU域内において個人データ処理の目的と手段に関する決定が行われる場所です1。主たる事業所は、管理者または処理者の越境処理活動の主導機関となる国の監督機関、および紛争や苦情が発生した場合に適用される国の法律を決定します2。各国監督機関、欧州データ保護監督機関、欧州委員会の代表者で構成される諮問機関である第29条作業部会は、GDPRに基づく管理者または処理者の主たる事業所の特定方法に関するガイドラインを発行しています3。このガイドラインでは、主たる事業所は、処理活動の実態と、それらの活動に対する管理権限

の有効かつ現実的な行使を反映しなければならないことを強調しています。ガイドラインはまた、「フォーラム・ショッピング」の慣行についても警告を発しています。これは、管理者または処理者が、意思決定やデータ処理の実際の所在地に関わらず、データ保護制度が最も柔軟または緩やかな加盟国に主たる拠点を指定する行為です。ガイドラインでは、このような慣行はGDPRで禁止されており、監督当局は管理者または処理者が主たる拠点を決定する際に用いる基準を綿密に監視・検証すると規定しています。監督当局は、主たる拠点が事実関係と一致していないと判断した場合、指定に異議を申し立て、関連する是正措置を適用することができます4。参考文献：GDPR第1条第4項(16) - 定義 - 一般データ保護規則（GDPR）
2 GDPR第56条～58条 - 協力と一貫性 - 一般データ保護規則（GDPR）3 ガイドライン
GDPR の地域的適用範囲に関する欧州データ保護会議規則 3/2018（第3 条）4 同上、14 ～ 15 ページ。

最新問題: **71**
ある企業は、安全とセキュリティ上の理由から、オフィスにCCTV監視カメラを設置したいと考えています。企業が依拠すべき法的根拠として最適なものは次のうちどれでしょうか？
A. 公的権力の行使。
B. 個人の同意
C. 正当な利益。
D. 公共の利益。
Answer: D (メーッセージを残す**)**

最新問題: **72**
スタートアップ企業MagicAIは、皮膚がんを検出する医療機器に搭載されるAIシステムを開発しています。AIシステムにおける潜在的なバイアス対策として、ITチームはユーザーの民族的出身、国籍、性別に関するデータを収集することを決定しました。
GDPR 第 9 条 (特別なカテゴリの個人データの処理) に基づくこの処理の最も適切な法的根拠はどれでしょうか?
A. 科学的または統計的目的のために必要な処理。
B. 重大な公共の利益のために必要な処理。
C. 予防医学または産業医学の目的のために必要な処理。
D. 過失の可能性がある事件における法的請求の防御のために必要な処理。
Answer: A (メーッセージを残す**)**
GDPR第9条は、人種や民族的起源を明らかにするデータを含む特別なカテゴリーの個人データの処理に関する厳格な条件を定めています。選択肢B、C、Dは関連性があるように見えるかもしれませんが、MagicAIのデータ収集の本質的な目的とは完全には一致していません。
オプション A が最も適切である理由は次のとおりです。
科学研究：MagicAIは、AIシステムの精度と公平性を向上させることを目指しており、人種、国籍、性別の違いによるパフォーマンスの違いを理解することで、AIシステムの精度と公平性の向上を目指しています。これは、医療の質の向上と医療技術におけるバイアスの低減を目指す科学研究に直接結びついています。
重要なのは、法的根拠として「科学的研究」を採用しているとしても、MagicAI は次のような厳格な安全対策を遵守する必要があるということです。
データ最小化: 研究に絶対に必要なデータのみを収集します。
目的の制限: 定義された科学的目的にのみデータを使用します。
適切なセキュリティ対策: 不正アクセスや漏洩からデータを保護します。

倫理審査: 理想的には、研究プロジェクトに対する倫理的承認を得ること。
参考文献:
GDPR第9条 - 特別なカテゴリーの個人データの処理
GDPR 序文 159 - 科学研究目的での特別なカテゴリのデータの処理条件 IAPP CIPP/E 教科書、第 2 章: 主要なデータ保護原則 (特に、特別なカテゴリのデータに関するセクション)

最新問題**: 73**
シナリオ
次の質問に答えるには、以下を使用してください。
ベッドロック保険の長年の顧客であるルイさんは、数か月前に軽い自動車事故に遭いました。
怪我人はいなかったものの、ルイスさんは 『アクシデンタブル」という会社から、人身傷害の賠償金回収を申し出るメッセージや電話に悩まされています。保険会社が顧客のデータを第三者に販売していると聞いており、ルイスさんはアクシデンタブルがベッドロック保険から自分の情報を入手したに違いないと確信しています。
ルイはまた、ベッドロック社からあらゆる種類の保険を売りつけようとするマーケティング情報をますます多く受け取るようになった。
これに動揺したルイは、インターネットの価格比較サイトを調べ始めました。長年ベッドロックの忠実な顧客であったにもかかわらず、他の保険会社がベッドロックよりもはるかに安い保険料を提示していることに気づき、衝撃を受けました。ベッドロックの保険の更新時期が来たとき、彼はザントルム保険に乗り換えることにしました。
新しい保険契約を有効にするには、ルイは無事故割引、車両、運転履歴に関する情報をZantrumに提供する必要があります。GDPRに基づく自身の権利を調べた後、彼はBedrockに対し、自身の情報をZantrumに直接転送するよう依頼する書面を提出しました。また、この機会に、Bedrockに対し、マーケティング目的での個人データの使用を停止するよう要請しました。
Bedrock は Louis に、PDF および XML (拡張マークアップ言語) バージョンの無保険証明書を提供しますが、技術的に不可能であるため Louis のデータを Zantrum に直接転送することはできないと伝えます。
ベッドロックはさらに、ルイの契約書には、ルイが自分のデータがマーケティング目的で使用されることに同意するという条項が含まれていたと説明する。ベッドロックによると、ルイがこの件について考えを変えるにはもう遅すぎるという。契約書の文言は法律用語だらけで非常に分かりにくかったため、ルイはそれを思い出して憤慨する。
その間も、ルイはアクシデンタブル -インシュアランスから迷惑電話を受け続けています。彼はアクシデンタブル -インシュアランスに手紙を書き、自分の個人情報を提供した組織の名前を尋ねました。彼はアクシデンタブル -インシュアランスが自分のデータを不法に使用していると考えており、データ保護当局に苦情を申し立てるつもりだと警告しました。手紙には、いかなる形であれ自分のデータがアクシデンタブル -インシュアランスに利用されることを望まない旨が記されていました。
アクシデンタブルからの返信は、ルイの疑念を裏付けるものでした。アクシデンタブルはベッドロック -インシュアランスの完全子会社であり、ルイが事故の保険金請求を提出した直後にベッドロックからルイの事故に関する情報を受け取りました。アクシデンタブルは、ルイの契約書にビジネス目的でベッドロックの関連会社と情報を共有することに同意する条項が含まれていたため、GDPR違反はないとルイに保証しました。
ルイはベッドロック社による扱いに嫌悪感を抱き、自分の情報をすべてコンピューター システムから消去するよう要求する手紙をベッドロック社に送りました。
ルイのデータポータビリティ要求に関する Bedrock の義務を正確に要約している記述はどれですか?
A. Bedrock は、Louis のデータを Zantrum に転送する義務を遵守していません。この義務は、個人データが自動化された手段によって処理され、顧客との契約の履行に必要な場合に適用されるためです。

B. 個人データが公共の利益のために処理される場合にはデータ移植権は適用されないため、Bedrock は Louis のデータを Zantrum に転送する必要はありません。
C. Bedrock は、すべての顧客データを要求に応じて他の保険会社に移植できるように、一般的に使用され、機械で読み取り可能で相互運用可能な形式を開発する義務があるため、Louis のデータを Zantrum に転送する義務を遵守していません。
D. 技術的に不可能な場合、Bedrock には Louis のデータを Zantrum に転送する義務はありません。
Answer: B (メーッセージを残す)

最新問題: **74**
シナリオ
次の質問に答えるには、以下を使用してください。
Wonderkidsは、託児サービスのオンライン予約サービスを提供しています。Wonderkidsはフランスに拠点を置いていますが、ウェブサイトはスイスの企業を通じて運営されています。サービスの一環として、Wonderkidsは、提供されたすべての個人データを、自社のシステムを通じて予約された託児サービス提供者に提供します。ウェブサイトで収集される個人データの種類には、託児サービスを予約した人の氏名、住所、連絡先、そして保育を受ける子供の氏名、年齢、性別、健康情報が含まれます。Wonderkidsのウェブサイトのプライバシーに関する声明には、次のように記載されています。
WonderkKidsは、本ウェブサイトを通じてお客様からご提供いただいた情報を、スケジュール管理および健康 ·安全上の理由から、お客様の保育サービス提供者に提供します。また、お客様およびお子様の個人情報を当社の正当な事業目的で使用する場合があり、データの保管にはスイスに所在する第三者ウェブサイトホスティング会社を利用しています。スイスに所在する機器に保管されるデータは、お客様およびお子様の個人情報の適切な保護を保証するための欧州委員会の規定を満たしています。
当社は、お客様とお子様の個人情報を、お客様に真の価値を提供できると判断する企業とのみ共有いたします。個人情報をご提供いただくことで、お客様は、関連企業への情報提供およびプロモーション情報の送付に同意するものとします。
当社は、お客様とお客様のお子様の個人情報を最長 28 日間保持することがあります。その時点でデータは匿名化されます。ただし、お客様の個人情報が 28 日を超えて正当な事業目的で使用される場合は、最長 2 年間保持されることがあります。
当社は、お客様およびお子様の個人情報をお客様の同意を得て処理しております。特定の情報をご提供いただけない場合、当社のサービスをご利用いただけない場合があります。お客様には、お客様およびお子様の個人情報へのアクセスを要求する権利、お客様またはお子様の個人情報を訂正または消去する権利、お客様および/またはお子様の個人情報の訂正または消去を求める権利、お客様およびお子様の個人情報の処理に異議を申し立てる権利があります。また、当社のデータ処理活動について監督当局に苦情を申し立てる権利もあります。WonderKidsとホスティングサービスプロバイダー間の契約には、どのような内容を含める必要がありますか？
A. データを保護するための技術的および組織的な対策を実施する要件。
B. コントローラー間モデル契約条項。
C. データ主体の監査権限。
D. 秘密保持契約。
Answer: (解答を表示する)
GDPR（一般データ保護規則）は、EU居住者の個人データを処理するすべての組織に適用されます。処理場所の如何に関わらず適用されます。したがって、フランスに拠点を置くデータ管理者であるWonderKidsは、WonderKidsに代わってデータ処理者として機能しているスイスのホスティングサービスプロバイダーに個人データを転送する際に、GDPRを遵守する必要があります。
GDPR第28条に基づき、データ管理者は、データ主体の権利保護とデータのセキュリティを確保するために、適切な技術的および組織的措置を実施する十分な保証を提供するデータ処理者のみを利用しなければなりません。また、データ管理者とデータ処理者は、

処理の対象、期間、性質、目的、ならびにデータ管理者の義務と権利を規定した書面による契約またはその他の法的行為を締結しなければなりません。
契約には、とりわけ以下の規定を含める必要があります。
* データ処理者は、EU または加盟国の法律で義務付けられている場合を除き、第三国または国際機関への個人データの転送を含め、データ管理者からの文書化された指示に従ってのみ個人データを処理する必要があります。
* データ処理者は、個人データを処理する権限を与えられた者が機密保持を約束しているか、または適切な法的機密保持義務を負っていることを保証する必要があります。
* データ処理者は、処理のセキュリティに関連する GDPR の第 32 条に従って必要なすべての措置を講じる必要があります。
* データ処理者は、他の処理者を雇用するための条件を尊重し、他の処理者の追加または置き換えに関する変更を予定している場合はデータ管理者に通知し、データ管理者にそのような変更に異議を申し立てる機会を与えなければなりません。
* データ処理者は、処理のセキュリティ、個人データ侵害の通知、個人データ侵害のデータ主体への伝達、データ保護影響評価、監督当局との事前協議に関連する、GDPR の第 32 条から第 36 条に従った義務の遵守を保証するためにデータ管理者を支援する必要があります。
* データ処理者は、データ管理者の選択により、処理に関連するサービスの提供終了後にすべての個人データを削除するかデータ管理者に返却し、EUまたは加盟国の法律で個人データの保管が義務付けられていない限り、既存のコピーを削除する必要があります。
* データ処理者は、GDPR 第 28 条に規定された義務の遵守を証明するために必要なすべての情報をデータ管理者に提供し、データ管理者またはデータ管理者が義務付けた別の監査人が実施する検査を含む監査を許可し、これに協力する必要があります。
したがって、4 つのオプションのうち、WonderKids とホスティング サービス プロバイダー間の契約に含める必要があるのは、データを保護するための技術的および組織的対策を実施するという要件です。これは、GDPR の第 28 条および第 32 条に基づくデータ処理者の義務の一部です。
その他の選択肢はGDPRでは必須ではありませんが、状況によっては推奨または望ましい場合があります。コントローラー間モデル契約条項は、個人データがデータコントローラーからデータプロセッサーへではなく、あるデータコントローラーから別のデータコントローラーへ転送される場合に使用されます。
GDPRではデータ主体の監査権は明示的に要求されていませんが、データ管理者は、データ処理者がデータ管理者またはデータ管理者が委託した他の監査人による監査を許可し、その監査に協力することを確保する必要があります。秘密保持契約は個人データの機密性を保護する上で有用ですが、データ処理関係のあらゆる側面を網羅しているわけではないため、GDPRの遵守を確保するには不十分です。
参考文献:
* GDPR
* ウェブホスティングとGDPRコンプライアンス - 注目すべき点
* GDPR: サードパーティのサービスプロバイダーのセキュリティを確認する必要がある理由
* サードパーティサービスプロバイダーのGDPRコンプライアンス :ベンダー管理

最新問題**: 75**
スペインの雇用主が従業員の個人データを毎年国の税務当局に送信する場合、どの GDPR 原則に最も依存するでしょうか?
A. 従業員の同意。
B. 雇用主の法的義務。
C. 行政の正当な利益。
D. 従業員の重大な利益の保護。

Answer: B (メーッセージを残す)
GDPR 第 6 条によれば、個人データの処理は、以下の少なくとも 1 つが当てはまる場合にのみ合法となります。
データ主体が、1 つ以上の特定の目的のために自身の個人データを処理することに同意している場合、データ主体が当事者である契約の履行のために、または契約締結前にデータ主体の要求に応じて措置を講じるために処理が必要な場合、コントローラーが負う法的義務を遵守するために処理が必要な場合、データ主体または他の自然人の重要な利益を保護するために処理が必要な場合、公共の利益のために実行されるタスクの履行またはコントローラーに付与された公的権限の行使のために処理が必要な場合、コントローラーまたは第三者が追求する正当な利益のために処理が必要な場合 (ただし、そのような利益が、個人データの保護を必要とするデータ主体の利益または基本的な権利および自由によって無効にされる場合は、特にデータ主体が子供である場合)。
In this case, the Spanish employer would most likely depend on the legal obligation of the employer as the lawful basis for sending the personal data of its employees to the national tax authority. This is because the employer is subject to the tax laws and regulations of Spain, which require the employer to report the income and deductions of its employees to the tax authority on an annual basis. The employer must comply with this legal obligation, and the processing of the employees' personal data is necessary for this purpose. The employer does not need to obtain the consent of the employees, as consent is not a valid basis for processing personal data where there is a clear imbalance between the data subject and the controller, such as in the context of employment. The employer also does not need to rely on the legitimate interest of the public administration, as this is not a specific purpose for which the employer is processing the personal data, but rather a general interest that may be served by the tax authority. The employer also does not need to invoke the protection of the vital interest of the employees, as this basis only applies in situations where the processing is necessary to protect someone's life, such as in a medical emergency. Reference: Article 6 GDPR - Lawfulness of processing - General Data Protection Regulation (GDPR), Lawful basis for processing | ICO, Legal obligation as a lawful basis for processing personal data under the GDPR, [Consent in the employment context | ICO], [Vital interests | ICO]

最新問題: **76**
従業員が雇用主に対して、自分に関して保有されている個人データへのアクセスを要求した場合、何が当てはまりますか?
A. 雇用主は、リクエストに第三者の個人データが含まれている場合、リクエストを自動的に拒否できます。
B. 情報が電子的にのみ保持されている場合、雇用主は要求を拒否できます。
C. 雇用主は従業員に関して保有するすべての情報を提供する必要があります。
D. 免除が適用されない限り、雇用主は従業員に関して保持されているすべての情報を提供する必要があります。
Answer: (解答を表示する)
説明

最新問題: **77**
ある組織が、自身の個人データに関する権利を行使しようとするデータ主体から、複数回のリクエストを受け取りました。どのような条件の下で、組織はデータ主体に対し、リクエストの処理費用を請求できますか？

A. 複数のリクエストがあったため、組織がそうすることが合理的であることを証明できる場合のみ。
B. GDPR の第 23 条に基づいて導入されたデータ主体の権利に対する制限の下で許可される範囲のみです。
C. 要求されたアクションを実行するための管理コストが特定のしきい値を超える場合のみ。
D. 組織が要求が明らかに過剰または誤っていることを証明できる場合のみ。
Answer: D (メーッセージを残す**)**
1. 明確な目的がない場合、明らかに軽薄または迷惑な場合、同一のデータ主体から繰り返し要求された場合、またはデータ主体の要求を満たすために合理的に必要な範囲を超えている場合、要求は明らかに根拠がない、または過剰である可能性があります2。このような場合、組織は合理的な手数料を請求するか、要求への対応を拒否することができますが、その決定の正当性を示すことができ、データ主体にその理由と監督機関への苦情申し立てまたは司法救済を求める権利を通知できなければなりません1。その他の選択肢は、GDPRにおける手数料請求の条件を反映していないか、または質問に関連しないため、正しくありません。参考文献 :アクセス権 | ICO、GDPRにおけるデータ主体の要求に対する手数料 - GDPR Wiki

最新問題**: 78**
データ保護責任者を任命した後、データ管理者またはデータ処理者にはどのような義務がありますか?
A. データ保護責任者が定義されたタスクの遂行に関して十分な指示を確実に受けられるようにするため。
B. データ保護責任者の定義されたタスクを実行し、専門知識を維持するために必要なリソースを提供します。
C. データ保護担当者が個人の質問に対する唯一の連絡先として機能することを保証するため:
個人データについて。
D. 組織の慣行を管理し、データ保護の原則への準拠を証明するための行動規範をデータ保護責任者に提出し、承認を得る。
Answer: B (メーッセージを残す**)**
英国GDPRによれば、管理者および処理者は、データ保護責任者が第39条に規定する業務を遂行できるよう、当該業務の遂行に必要なリソース、個人データおよび処理業務へのアクセス、ならびにデータ保護責任者の専門知識の維持に必要なリソースを提供することにより、データ保護責任者を支援しなければならない1。また、管理者および処理者は、データ保護責任者がこれらの業務の遂行に関していかなる指示も受けないこと、およびデータ保護責任者が管理者または処理者の最高経営責任者に直接報告することを確保しなければならない1。

最新問題**: 79**
ある多国籍企業が、義務的なデータ保護責任者（DPO）を任命しています。GDPR第37条（1）に定められた規則を考慮することに加え、事業を展開するすべてのEU加盟国・地域におけるコンプライアンスを確保するために、企業は以下のどの措置を講じる必要がありますか？
A. 国内の特例を参照して、この問題に関して検討すべき追加のケースがあるかどうかを評価します。
B. 会社が事業を展開するすべての国における処理業務について、データ保護プライバシー評価を実施します。
C. 企業が設立されている EU 加盟国のそれぞれに 250 人を超える従業員がいるかどうかを評価します。
D. Revise the data processing activities of the company that affect more than one jurisdiction to evaluate whether they comply with the principles of privacy by design and by default.
Answer: A (メーッセージを残す**)**
A multinational company that is appointing a mandatory data protection officer (DPO) must also consult national derogations to evaluate if there are additional cases to be considered in relation to the matter. According to Article 37 (1) of the GDPR, a DPO must be designated by the controller or the processor in any case where: (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing

operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences 1. However, Article 37 (4) of the GDPR also allows Member States to provide for additional cases where a DPO must be designated by law 1. Therefore, a multinational company must consult the national laws of the EU jurisdictions in which it operates to ensure that it complies with any additional requirements for appointing a DPO.
The other options are not correct because they are not directly related to the appointment of a DPO. Conducting a Data Protection Privacy Assessment, assessing the number of employees, and revising the data processing activities are all good practices for ensuring compliance with the GDPR, but they are not mandatory actions for designating a DPO. Moreover, the number of employees is not a relevant criterion for appointing a DPO, as the GDPR does not set any threshold based on the size of the organization 2. Reference: 1: Article 37 of the GDPR 2: Guidelines on Data Protection Officers ('DPOs')

最新問題**: 80**
2018 年に改正された次の条約 108+ の原則のうち、GDPR の原則と一致しないものはどれですか。
A. データ侵害を申告する企業の義務。
B. 監督機関へのコンプライアンスを証明する要件。
C. 政府による個人データの大量収集の必要性。
Answer: (解答を表示する**)**
参考 :https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018PC0449&from=HU

最新問題**: 81**
スポーツ アパレルおよびトロフィー会社の最高マーケティング責任者であるジェリーは、世界中の学校や運動クラブに製品を販売しています。最近、この会社はカスタマイズされたスポーツ用具の新製品ラインに投資することを決定しました。ジェリーは、現在の顧客ベースに電子メールを送信して、そのような用具の初回購入時に割引を提供する予定です。
ジェリーはプライバシー担当ディレクターのケイトに計画について話します。ケイトがジェリーに提供できる最善のアドバイスは何でしょうか？
A. ジェリーが既存の顧客に同様の製品を販売するという計画を実行することを許可します。
B. ジェリーが正当な利益に基づいてマーケティング計画を実行することを許可する
C. ジェリーに、現在の顧客全員にマーケティングメールの受信を希望する旨の2回目の通知を送信するよう要求する
D. 今後、マーケティングメールの配信を停止するオプションを Jerry に追加することを要求します。
Answer: C (メーッセージを残す**)**

最新問題**: 82**
EU 法に基づく権利の行使を希望する個人の行動について決定を下すのはどの司法機関ですか?
A. 会計検査院
B. 欧州連合司法裁判所
C. 欧州人権裁判所
D. 欧州データ保護委員会
Answer: B (メーッセージを残す**)**
参考 :https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_en

最新問題: **83**
EDPB（欧州データ保護局）のソーシャルメディア利用者のターゲティングに関するガイドライン8/2020では、個人データ処理の法的根拠として正当な利益に依拠するには、3つのテストに合格する必要があると規定されています。次の3つのテストのうち、どれが該当しませんか？
A. 目的テスト。
B. 必要性テスト。
C. バランステスト。
D. 適切性テスト。
Answer: D (メーッセージを残す**)**
EDPBのソーシャルメディアユーザーのターゲティングに関するガイドライン8/2020では、正当な利益の法的根拠には、目的テスト、必要性テスト、均衡テストという3つの累積的なテストに合格する必要があると説明されています。目的テストは、データ管理者または第三者が追求する正当な利益があるかどうかを検証します。必要性テストは、処理が特定された目的に必要かどうかを検証します。均衡テストは、正当な利益がデータ主体の利益または権利と自由によって上書きされないかどうかを検証します。十分性テストは、正当な利益の法的根拠に必要な3つのテストの1つではありません。十分性テストは、第三国へのデータ転送に関連し、EU内でのデータ処理には関連しません。
参照：
ソーシャルメディアユーザーのターゲティングに関するEDPBガイドライン8/2020、セクション3.2.11、GDPR第6条(1)(f)2、GDPR前文472、IAPP CIPP/E学習ガイド、第3章、セクション3.2.23

最新問題: **84**
GDPR の 個人データ」の定義に含まれない可能性が高いのは次のうちどれですか?
A. オランダ国民の支払いカード番号
B. フランスに住むアメリカ国民の米国社会保障番号
C. イタリアの企業が統計目的で使用したリンクされていない集計データ
D. ドイツの専門試験を受けるドイツ人の受験者の識別番号
Answer: (解答を表示する**)**
GDPRにおける個人データの定義は広範であり、特定された、または特定可能な自然人に関するあらゆる情報が含まれます。つまり、個人データには、氏名、メールアドレス、電話番号、住所、生年月日、人種、性別、政治的意見など、様々な情報が含まれます。GDPRは、あらゆるレベル、プラットフォーム、テクノロジーにおいて個人データを保護し、組織に対し、特定の目的にのみ個人データを処理し、一定期間保管することを義務付けています。
イタリア企業が統計目的で利用する、リンクされていない集計データは、GDPRにおける個人データの定義に該当しない可能性が高いでしょう。集計データとは、個々の記録を識別できなくなるように処理されたデータです。例えば、企業が顧客の名前とメールアドレスを収集し、平均年齢を計算する場合、その結果得られるデータは集計データであり、個人情報ではありません。したがって、この種のデータはGDPRの対象にはなりません。
しかし、これはイタリア企業がこの種のデータをいかなる制限や義務もなく使用できることを意味するものではありません。GDPRは、いかなる形式や方法においても個人データを伴うあらゆる処理活動に依然として適用されます。例えば、イタリア企業がこの種のデータを使用して、顧客の特性や嗜好に基づいて顧客のプロファイルやセグメントを作成する場合でも、GDPRに基づく特定の原則や条件に準拠する必要がある場合があります。例えば、顧客の集計データをマーケティング目的で使用する前に同意を得る必要が

ある場合や、集計データが正確かつ最新であることを保証する必要がある場合もあります。集計データの保持期間を制限する必要がある場合もあります。また、個人データに関する顧客の権利を尊重する必要がある場合もあります。
参照：
個人データとは何ですか？ | ICO
EU GDPR では何が個人データとみなされますか?
[GDPR 個人データ - どのような情報が対象になりますか?]

最新問題: **85**
米国を拠点とするニュース ウェブサイトは、主に北米の出来事を報道しています。ウェブサイトの運営者は米国外からの接続をブロックしていないため、ウェブサイトは場所に関係なくすべてのユーザーがアクセスできます。ウェブサイトは、ユーザー アカウントの作成を必要とする有料サブスクリプションを提供しており、このサブスクリプションの支払いは米ドルでのみ可能です。
アカウント作成とサブスクリプションに関連するすべての処理を担当するウェブサイト運営者が GDPR に準拠する必要がない理由を説明するのは次のうちどれですか。
A. このウェブサイトは、欧州連合加盟国のいくつかの公用語では利用できません。
B. ウェブサイトは、仮想プライベート ネットワーク (VPN) を使用して米国の場所をシミュレートする米国外からの接続をブロックできません。
C. 欧州連合通貨での支払いはできません。
D. 管理者は欧州連合内に拠点を持っていません。
Answer: D (メーッセージを残す**)**

最新問題: **86**
シナリオ
次の質問に答えるには、以下を使用してください。
ハビエルさんは、フィットネスクラブEVERFITの会員です。この会社は多くのEU加盟国に支店を持っていますが、GDPRの目的上、主要な事業所はフランスにあります。ハビエルさんは、北アイルランド（英国の一部）のニューリーに住んでおり、国境を越えてアイルランドのダンドークに通勤しています。2年前、出張中に、ハビエルさんはドイツのフランクフルトにあるEVERFITの支店でトレーニング中に写真を撮られました。当時、ハビエルさんは、写真は宣伝目的にのみ使用されると説明され、写真に写ることに同意しました。それ以来、その写真はクラブの英国版パンフレットに使用され、英国版ウェブサイトのランディングページにも掲載されています。しかし、このフィットネスクラブは最近、EU加盟国にあるクラブの様々な支店で会員に対する不当な扱いが蔓延したため、評判が悪くなっています。その結果、ハビエルさんは、自分の写真がフィットネスクラブと公に関連付けられることに不快感を覚えるようになりました。
この件について話し合うため、地元支店の支店長との面談予約を何度も試みたものの、うまくいかなかったハビエルはEVETFITに手紙を送り、ウェブサイトとすべての販促資料から自分の写真を削除するよう要請した。数ヶ月が経過しても、要請に対する返答がなかったハビエルは、この件について強い不安を抱くようになった。他の手段を用いてEVETFITに何度も連絡を取ろうとしたが、それでもうまくいかなかったため、彼はEVETFITに対して訴訟を起こすことを決意した。
ハビエルは、この件について英国情報コミッショナー事務局（ICO、英国の監督機関）に苦情を申し立てました。ICOは、GDPR第56条（3）に基づき、CNIL（EVERFITの主要拠点の監督機関）にこの件を通知しました。EVERFITは英国に拠点を有しているにもかかわらず、CNILはGDPR第60条に基づき、この件を処理することを決定しました。CNILは、協力手続きに基づき、ICOと連携しました。監督

機関間で決定に至る上での問題点を考慮し、欧州データ保護会議が関与し、一貫性メカニズムに基づき、拘束力のある決定を下しました。
さらに、ハビエルさんは、パンフレットとウェブサイトから自分の写真を削除するという要求をEVERFITが受け入れなかったことによる損害についてEVERFITを訴えている。
複数の EU 諸国にわたる複数の EVETFIT 支部が別々のデータ管理者として機能し、各支部が Javier の要求を不適切に処理した責任があると仮定した場合、Javier は補償を求めるためにどのような手続きを取ることができますか?
A. 各支部が全損害に対して責任を負う可能性があるため、彼は関連する EVETFIT 支部のいずれかを訴えることができます。
B. ハビエルは、各 EVETFIT 支部を訴え、各支部がハビエルが被った損害や苦痛への貢献度に応じて比例した補償金を支払うようにしなければなりません。
C. 彼は、欧州データ保護委員会の決定に基づいて、どの EVETFIT 支部が損害賠償責任を負うのかを決定するために、欧州データ保護委員会に申請することができます。
D. 彼は、EVETFIT の主要拠点があるフランスにある EVETFIT 本社を訴える必要があるでしょう。
Answer: D (メーッセージを残す**)**

最新問題**: 87**
次のどれがクラウド コンピューティング サービスの共通の特性として認識されていませんか?
A. サービスのインフラストラクチャはサプライヤーの顧客間で共有され、複数の国に配置される場合があります。
B. サプライヤーは、処理に適用される場所、セキュリティ対策、およびサービス基準を決定します。
C. サプライヤーは、容量に応じて顧客データをインフラストラクチャ内で転送することを許可します。
D. サプライヤーは、サプライヤーによって処理されるデータに関連するベンダーのビジネスリスクを負います。
Answer: D (メーッセージを残す**)**
これはクラウドコンピューティングサービスに共通する特徴ではありません。なぜなら、サプライヤーは通常、ベンダーの事業リスクを負わないからです。実際、サプライヤーはデータ漏洩や損失に対する責任を制限することが多く、ベンダーはデータ保護に関する法令遵守の責任を負います。その他の選択肢は、クラウドコンピューティングが柔軟で拡張性が高く、費用対効果の高いデータ処理方法であるという性質を反映している一方で、データ保護とセキュリティの面で課題も抱えているため、クラウドコンピューティングサービスの一般的な特徴です。参考文献：
* 無料のCIPP/E学習ガイド、17ページ、セクション2.3.2
* CIPP/E認証、12ページ、セクション2.3.2
* Cipp-e 学習ガイド、授業ノートと要約、23 ページ、セクション 2.3.2

最新問題**: 88**
ある多国籍企業が、義務的なデータ保護責任者（DPO）を任命しています。GDPR第37条（1）に定められた規則を考慮することに加え、事業を展開するすべてのEU加盟国・地域におけるコンプライアンスを確保するために、企業は以下のどの措置を講じる必要がありますか？
A. 国内の特例を参照して、この問題に関して検討すべき追加のケースがあるかどうかを評価します。
B. 複数の管轄区域に影響を及ぼす会社のデータ処理活動を改訂し、設計およびデフォルトでプライバシーの原則に準拠しているかどうかを評価します。
C. 会社が事業を展開しているすべての国における処理業務について、データ保護プライバシー評価を実施します。
D. 企業が設立されている EU 加盟国のそれぞれに 250 人を超える従業員がいるかどうかを評価します。

Answer: (解答を表示する**)**

最新問題**: 89**
GDPR 第 14 条によれば、データ主体の個人データが他の情報源から取得された場合、管理者はデータ主体に必要なプライバシー情報をどのくらいの期間提供する必要がありますか?
A. 個人情報を取得後、できるだけ早く。
B. データ主体との最初のコミュニケーション後、できるだけ早く。
C. 個人情報を取得してから合理的な期間内に、遅くとも1か月以内に行います。
D. 個人データを取得してから合理的な期間内ですが、8週間以内です。
Answer: C (メーッセージを残す**)**
参照 :https://dataprivacymanager.net/gdpr-exemptions-from-the-obligation-to-provide-information-to-the-individual-data-subject/

最新問題**: 90**
欧州委員会が今後これと異なる決定を下すまで、GDPR に基づく適正ステータスを引き続き享受できる国は次のうちどれですか?
A. ギリシャ
B. ノルウェー
C. オーストラリア
D. スイス
Answer: D (メーッセージを残す**)**
十分性とは、EUがEU域内におけるデータ保護と 実質的に同等」の水準のデータ保護を提供しているとみなす他の国、地域、セクター、または国際機関を指す用語です。十分性認定とは、EUが行う正式な決定であり、他の国、地域、セクター、または国際機関がEUと同等の水準の個人データ保護を提供していることを認めるものです。この認定の結果、EU およびノルウェー、リヒテンシュタイン、アイスランド）から当該第三国への個人データの移転は、追加の保護措置を必要とせずに可能となります12。
欧州委員会は、これまでにアンドラ、アルゼンチン、カナダ（商業組織）フェロー諸島、ガーンジー、イスラエル、マン島、日本、ジャージー島、ニュージーランド、大韓民国、スイス、GDPRおよびLEDに基づく英国、米国 EU-米国間データプライバシーフレームワークに参加している商業組織）、ウルグアイが適切な保護を提供していると認定している13。2021年6月28日、EU委員会は英国に関する2つの十分性決定を公表した。1つはEU GDPRに基づく移転に関するもので、もう1つは法執行指令 LED）に基づく移転に関するものである2。これらの決定には、欧州委員会による英国の個人データ保護法とシステムの詳細な評価、および英国を十分であると指定する法律が含まれている。両方の十分性決定は、2025年6月27日まで有効と予想される2。
4つの選択肢のうち、スイスのみがEUから十分性認定を受けており、これは、欧州委員会が今後これと異なる決定を下すまで、GDPRに基づく十分性認定を引き続き享受することを意味します。ギリシャはEU加盟国であるため、EUから個人データを受け取るために十分性認定を受ける必要はありません。ノルウェーは、アイスランドとリヒテンシュタインを含む欧州経済領域 EEA）の加盟国であり、GDPRを国内法に組み入れているため、十分性認定を受ける必要はありません。オーストラリアはEUから十分性認定を受けていないため、EUからオーストラリアへの個人データの移転には、適切な保護措置または例外措置が必要です13。したがって、正解はD. スイスです。参考：
https://pages.iapp.org/Free-Study-Guides_CIPPE-PPC-EU.html https://data-privacy-office.eu/courses/cipp-e-official-training-course/

最新問題**: 91**
欧州人権裁判所 (ECHR) と欧州連合司法裁判所 (CJEU) の役割と機能に関する重要な違いは何ですか?
A. ECHR は基本的権利としてのプライバシーに関する問題について判決を下すことができますが、CJEU はそれができません。

B. CJEU は各国政府に EU 法を実施し尊重するよう強制できますが、ECHR はそれができません。
C. CJEU は国内裁判所による人権判決に対する控訴を審理できますが、ECHR は審理できません。
D. ECHR は人権法を実施しない政府に対して人権法を強制執行できますが、CJEU はそれができません。
Answer: B (メーッセージを残す**)**
ECHR と CJEU は、それぞれ欧州評議会と欧州連合という異なる法体系の一部です。ECHR は、47 の加盟国の管轄権内の個人に対して人権と基本的自由を保証する条約です。CJEU は、27 の加盟国における EU 法の統一的な解釈と適用を確保する EU の司法機関です。ECHR は、条約で保障された権利の侵害を主張する個人または国家からの苦情のみを審理し、被告国を拘束する判決のみを下すことができます。一方、CJEU は、EU 法のあらゆる問題に関して、個人、国家、EU 機関、または国内裁判所からの訴訟を審理し、すべての EU 加盟国および機関を拘束する判決を下すことができます。CJEU はまた、判決または EU 法全般に従わない国家に制裁や罰則を課すことができます。したがって、欧州人権裁判所（CJEU）は、欧州人権裁判所（ECHR）が人権法を執行するよりも、EU法を執行する上でより大きな権限と権限を有しています。参考：CIPP/E認証、欧州人権裁判所と欧州司法裁判所、英国、EU、そして英国権利章典

最新問題: **92**
ある企業が、欧州連合/EEA 以外の国に個人データを転送したいと考えています。そのために、その国の法律と慣行の評価を計画していますが、これらが自社が使用しようとしている転送保護手段に影響を及ぼす可能性があることを承知しています。次のすべての要素は、企業が検討する必要がある要素のうち、どれを除くか?
A. 欧州連合に設立されたデータ管理者または処理者との間の契約条項
/EEAおよび関係する第三国に設立された移転の受取人
B. 同一または別の第三国のサブプロセッサーへの個人データの転送など、あらゆる転送。
C. 移転される個人データにアクセスする可能性のある第三国の当局が利用できる技術的、財政的、および人的資源
D. 関係する第三国における近代化のプロセスと、個人データの国際移転に依存する新興技術へのアクセス
Answer: D (メーッセージを残す**)**

最新問題: **93**
欧州データ保護委員会 (EDPB) は、転送ツールが欧州連合 (EU) レベルに準拠した個人データ保護レベルを効果的に提供しているかどうかの再評価をいつ推奨しますか?
A. 個人データ漏洩後。
B. 3年ごと。
C. 継続的に。
D. 毎年です。
Answer: (解答を表示する**)**
参照：

EDPB の EU の個人データ保護レベルへの準拠を確保するための移転ツールを補完する措置に関する勧告 01/2020」によれば、第三国への個人データの輸出者は、移転する個人データの保護レベルに影響を及ぼす可能性のある第三国における動向を継続的に監視する必要があります1。つまり、輸出者は、標準契約条項、拘束的企業準則、行動規範、認証メカニズムなど、依存する移転ツールが、EU レベルに準拠した個人データ保護レベルを効果的に提供しているかどうかを再評価する必要があります。EDPB は、輸出者がこの再評価と、その結果生じる変更を文書化することを推奨しています1。EDPB はこの再評価の固定期間を指定しておらず、各移転の特定の状況と第三国における関連する動向を考慮に入れながら、継続的に行う必要があると述べています。
1 :EUの個人データ保護レベルへの準拠を確保するための転送ツールを補完する措置に関するEDPB勧告01/2020、バージョン2.0、2021年6月18日に採択、パラグラフ85〜86。

最新問題: **94**
欧州データ保護指令 95/46/EC の目的は何でしたか?
A. 欧州人権条約の実施をすべての加盟国間で調和させること。
B. プライバシーの保護と個人データの国境を越えた流れに関する OECD ガイドラインを実施する。
C. 個人データが欧州連合外に転送されるのを完全に防止します。
D. 個人の基本的権利の保護と、加盟国間でのデータの自由な流れをさらに調和させる。
Answer: D (メーッセージを残す**)**
参照 https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (3)

最新問題: **95**
シナリオ
次の質問に答えるには、以下を使用してください。
Building Block Inc.はシカゴに本社を置き、米国、アジア、ヨーロッパ (ドイツ、イタリア、フランス、ポルトガルを含む)にオフィスを構える多国籍企業です。昨年、同社はフィッシング攻撃の被害に遭い、大規模なデータ漏洩が発生しました。取締役会は、ゼネラルマネージャー、プライバシーオフィス、情報セキュリティチームと連携し、追加のセキュリティ対策を講じることを決議しました。これには、トレーニングによる意識向上プログラム、サイバーセキュリティ監査、そしてSecurityScanと呼ばれる新しいソフトウェアツールの導入が含まれます。SecurityScanは、従業員のコンピュータをスキャンし、ベンダーによるサポートが終了してセキュリティアップデートが提供されていないソフトウェアがないか確認します。このソフトウェアは、従業員のコンピュータの監視など、他の機能も備えています。
これらの対策は従業員に影響を及ぼす可能性があるため、Building Block のプライバシー オフィスは、情報セキュリティを強化し、将来のデータ侵害を防止するための一連の取り組みを実施することを通知する一般通知を全従業員に発行することを決定しました。
これらの対策を実施した後、サーバーのパフォーマンスが低下しました。ゼネラルマネージャーは、セキュリティチームに対し、SecurityScanを使用して従業員のコンピュータのアクティビティと位置情報を監視する方法を指示しました。
これらの活動の中で、情報セキュリティチームは、イタリア出身の従業員が映画のビデオライブラリに毎日接続していること、またドイツ出身の従業員が許可なくリモートワークを行っていることを発見しました。セキュリティチームはこれらのインシデントをプライバシーオフィスとゼネラルマネージャーに報告しました。報告書の中で、チームはイタリア出身の従業員がサーバーのパフォーマンス低下の原因であると結論付けました。

これらの違反行為の重大性を考慮し、同社のセキュリティおよびプライバシーポリシーでは、従業員が会社のコンピュータにソフトウェアをインストールしたり、許可なくリモートワークしたりすることを禁止しているため、同社は両従業員に懲戒処分を適用することを決定しました。
Building Block がイタリア人従業員の状況に対処する最も適切な方法は何でしょうか?
A. この状況には GDPR は適用されないため、会社にはイタリアの労働法で認められている懲戒処分を適用する権利があります。
B. 当該従業員はサーバーのパフォーマンスとデータに重大なリスクを引き起こしたため、会社は当該従業員に対して公正解雇を含む懲戒処分を適用する権利を有します。
C. セキュリティ対策が監視などの他の目的に使用されることが従業員に通知されていなかったため、会社はこの従業員に対して懲戒処分を適用することが困難になる可能性があります。
D. これは重大な違反であったが、従業員は新しいセキュリティ対策の結果について適切に知らされていなかったため、会社は懲戒処分を適用する権利はあるものの、解雇する権利はない。
Answer: (解答を表示する**)**
GDPRによれば、監視ソフトウェアを通じて取得された個人データの処理は、合法、公正、かつ透明でなければなりません。つまり、雇用主は従業員に対し、監視の性質、範囲、理由、そして会社のポリシーに違反した場合に起こり得る結果について通知しなければなりません。また、雇用主は従業員のデータを処理する正当な利益またはその他の法的根拠を有し、従業員の権利と自由を尊重しなければなりません。さらに、雇用主は事業を展開する各加盟国の国内法およびガイドラインを遵守する必要があり、これらの法律およびガイドラインは従業員の監視に追加の条件や制限を課す可能性があります。本件において、Building Block社はイタリアの従業員に対し、セキュリティソフトウェアが従業員のコンピュータの活動や位置情報も監視することを通知しておらず、そのような監視の目的と範囲も明示していませんでした。したがって、従業員は自分の個人データがこのように処理されることを合理的に予想できず、GDPRに基づく権利（アクセス、訂正、処理への異議申し立てなど）を行使することもできませんでした。さらに、雇用主は監視の必要性と比例性について適切な評価を行わず、セキュリティ目標を達成するためのより侵害の少ない代替手段を検討していませんでした。そのため、雇用主が監視ソフトウェアを通じて得られたデータに基づいて懲戒処分を決定した場合、従業員、イタリアの監督当局、または労働裁判所から法的訴訟を受ける可能性があります。また、雇用主はGDPRおよびイタリアのデータ保護法に違反したとして罰金または制裁を受ける可能性があります。参考資料：従業員監視に関するGDPR要件：遵守すべきルール、組織は従業員の個人的なコミュニケーションを監視できますか？、ICOが職場における合法的な監視を確保するためのガイダンスを公開、コネクテッドカーおよびモビリティ関連アプリケーションにおける個人データ処理に関するガイドライン

最新問題**: 96**
EDPB のガイドライン 4/2019 「第 25 条 データ保護の設計およびデフォルトに関するガイドライン」では、次のすべての慣行は、EU データ保護法に基づく個人データの処理に関する原則に従っていますが、次の例外はありません。
A. データ所有権の割り当て。
B. アクセス制御管理。
C. 頻繁な仮名化キーのローテーション。
D. 処理チェーンに沿ったエラーの伝播を回避します。
Answer: A (メーッセージを残す**)**
EDPB（欧州データ保護局）の「第25条 データ保護の設計とデフォルトに関するガイドライン 4/2019」は、GDPR第25条の要件をどのように実施するかについてのガイダンスを提供しています。この要件は、個人データの処理がデータ保護原則に準拠し、データ主体の権利と自由を保護することを保証するために、管理者に適切な技術的および組織的措置と必要な保護手段を設計および実施する

ことを義務付けています。このガイドラインではまた、デフォルトで処理の特定の目的に必要な個人データのみが処理されるという「デフォルトによるデータ保護」の概念の適用方法についても説明しています。
ガイドラインでは、EUデータ保護法に基づく個人データ処理に関する原則に基づく実務として、データ所有権の配分について言及されていません。データ所有権の配分は、GDPRやEDPBによって認識または定義されている概念ではありません。データ所有権の配分とは、データ主体またはデータ管理者が、提供または処理する個人データに対して何らかの形の財産権を有するという考え方を指します。
しかし、GDPRはそのような権利を付与するものではなく、管理者と処理者の説明責任と責任という概念に基づき、個人データの処理に関する一連の規則と義務を定めています。GDPRはまた、個人データの所有権ではなく、個人データがデータ主体に関連しているという事実に基づいて、アクセス、訂正、消去、制限、ポータビリティ、異議申し立て、自動化された意思決定の対象とならない権利など、データ主体の権利と自由を認めています。
質問に記載されているその他の実践、すなわちアクセス制御管理、頻繁な仮名化キーのローテーション、処理チェーン全体にわたるエラー伝播の回避は、ガイドラインで説明されているように、EUデータ保護法の下での個人データの処理に関する原則に従う実践例です。アクセス制御管理は完全性と機密性の原則に従います。この原則では、個人データが、許可されていないまたは違法な処理、および偶発的な損失、破壊、または損傷からの保護を含む、個人データの適切なセキュリティを確保する方法で処理されることが求められます。頻繁な仮名化キーのローテーションは、個人データが処理される目的に関連して適切で、関連性があり、必要なものに限定されることが求められます。処理チェーン全体にわたるエラー伝播の回避は正確性の原則に従います。この原則では、個人データが正確であり、必要に応じて最新の状態に保たれることが求められます。
参考文献:
GDPR、第5条、第6条、第7条、第8条、第9条、第15条、第16条、第17条、第18条、第19条、第20条、第21条、第22条および第25条。
EDPBガイドライン4/2019第25条データ保護設計とデフォルトに関する5、6、7、8、9、10、11ページ
12、13、14、15、16、17、18、19、20、21、22、23、24、25、26、27、28。

最新問題: **97**
Article 5(1)(b) of the GDPR states that personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes." Based on Article 5(1)(b), what is the impact of a member state's interpretation of the word "incompatible"?
A. It dictates the level of security a processor must follow when using and storing personal data for two different purposes.
B. It guides the courts on the severity of the consequences for those who are convicted of the intentional misuse of personal data.
C. It sets the standard for the level of detail a controller must record when documenting the purpose for collecting personal data.
D. It indicates the degree of flexibility a controller has in using personal data in ways that may vary from its original intended purpose.
Answer: D (メーッセージを残す)
The purpose limitation principle requires that personal data be collected for specified, explicit and legitimate purposes and not be further processed in a manner that is incompatible with those purposes. However, the GDPR does not provide a clear definition of what constitutes an incompatible purpose. Instead, it leaves room for interpretation by the member states, taking into account the context and circumstances of the processing.
This means that the degree of flexibility a controller has in using personal data for a new purpose may vary depending on the member state's law and guidance. Some factors that may affect the compatibility assessment include the link between the original and the new purpose, the expectations of the data subject, the nature of the data, the impact of the further processing, and the safeguards applied by the controller. References:

* GDPR Article 5(1)(b), which states the purpose limitation principle.
* GDPR Article 6(4), which lists the criteria for assessing the compatibility of a new purpose.
* ICO guidance, which explains the purpose limitation principle and provides examples of compatible and incompatible purposes.
* [EDPB guidelines], which provide further guidance on the application of the purpose limitation principle.

最新問題**: 98**
シナリオ
次の質問に答えるには、以下を使用してください。
TripBliss Inc.は、ここ数年で大幅な収益減少に陥っている旅行サービス会社です。新任マネージャーのオリバーは、その一因として会社のウェブサイトの老朽化が考えられます。調査を行った後、彼は新興IT企業Techivaの営業担当者と面談し、TripBliss Inc.の経営難に陥った事業のために、最先端のウェブサイトを新たにデザインしてくれることを期待します。
交渉中、Techiva の担当者は、詳細なアンケートを通じてより多くの顧客情報を収集する計画について説明しました。この情報は、顧客の好みを特定の旅行先に合わせて調整するために使用できます。
TripBliss Inc.は、年齢、収入、民族など、目標達成に最も役立つデータカテゴリーをいくつでも選択できます。オリバーはこのアイデアに満足していますが、アンケート調査では顧客からデータ収集への明示的な同意を得る必要があるため、このアプローチの成功度を測る方法も必要です。Techivaの担当者は、顧客がどのようにウェブサイトを利用しているかをより深く理解するために、新しいウェブサイトのトラフィックを分析するプログラムも実行することを提案しました。担当者は、顧客のデバイスに複数のCookieを配置する計画を説明します。これらのCookieにより、TripBliss Inc.はIPアドレスやその他の情報を収集できます。例えば、顧客がどのサイトからアクセスしたか、TripBliss Inc.のウェブサイトで過ごした時間、どのページを訪問したかなどです。これらの情報はすべてログファイルにまとめられ、Techivaが専用のプログラムで分析します。TripBliss Inc.は、ウェブサイトの効果を評価するために、集計統計情報を受け取ります。オリバーは、これらのサービスをTechivaに積極的に依頼しています。
Techiva社は、長年のアカウントマネージャーであるレオン・サントス氏に、プロジェクトの分析部分を委託しました。通常の業務手順通り、レオン氏にはTripBliss社のウェブサイトの管理者権限が与えられ、そこから収集されたログファイルへのアクセスを許可することができます。しかし、TripBliss社にとって残念なことに、レオン氏がこの新しいプロジェクトを引き受けたのは、Techiva社への不満が最高潮に達していた時期でした。会社から不当な扱いを受けたと感じたレオンは、復讐のため、趣味でハッカーをしている友人のフレッド氏に協力を求めます。二人は協力して、フレッド氏にTechiva社のシステムに侵入させ、ログファイルをUSBメモリにコピーするという計画を立てます。
当初、レオンはUSBメモリをマスコミとデータ保護当局に送り、Techiva社を告発するつもりだったが、良心の呵責に襲われ、計画を思いとどまる。USBメモリからすべてのデータを安全に消去し、会社のアクセス制御システムを見直す必要があると上司に伝えることにした。
TripBliss Inc. のウェブサイト Cookie の使用に関して、正しい記述は次のうちどれですか?
A. 関係するデータのカテゴリのため、Cookie の使用に関する明示的な同意を顧客から別途取得する必要があります。
B. クッキーを使用すると位置情報が追跡される可能性があるため、顧客から明示的な同意を得る必要があります。
C. Techiva は Cookie から収集されたデータの集計統計のみを受信するため、追加の同意は必要ありません。
D. TripBliss Inc. から要求されたサービスの使用を有効にするためにすべての Cookie が厳密に必要なわけではないため、Cookie の使用には同意要件が適用されます。
Answer: A (メーッセージを残す**)**

最新問題**: 99**

According to Article 14 of the GDPR, how long does a controller have to provide a data subject with necessary privacy information, if that subject's personal data has been obtained from other sources?
A. Within a reasonable period after obtaining the personal data, but no later than one month.
B. Within a reasonable period after obtaining the personal data, but no later than eight weeks.
C. As soon as possible after the first communication with the data subject.
D. As soon as possible after obtaining the personal data.
Answer: D (メーッセージを残す)

最新問題**: 100**
ほとんどのプロセッサーがデータ処理活動に関連して保持しなければならない記録に含める必要がないのは次のどれですか?
A. プロセッサが代理を務める各コントローラの名前と連絡先の詳細。
B. プロセッサが機能している各コントローラに代わって実行される処理のカテゴリ。
C. プロセッサが行動している各コントローラに代わって実行される第三国への個人データの転送の詳細。
D. プロセッサが代理を務める各コントローラに代わってプロセッサが実行する処理活動に関連して実施されたデータ保護影響評価の詳細。
Answer: D (メーッセージを残す)
GDPR によれば、処理者は各管理者に代わって実行されるすべてのカテゴリーの処理活動の記録を保持しなければならず、これには以下の情報が含まれます12。
処理者（複数可）処理者が代理を務める各管理者（該当する場合）、およびデータ保護責任者（該当する場合）の氏名と連絡先、各管理者に代わって実行される処理の種類、該当する場合、第三国または国際機関への個人データの移転（当該第三国または国際機関の識別情報を含む）、および第49条(1)項第2段落で言及されている移転の場合には、適切な保護措置の文書化、可能であれば、第32条(1)で言及されている技術的および組織的なセキュリティ対策の概要。
記録は書面（電子形式を含む）で作成され、監督機関の要請に応じて開示されなければなりません。記録保持義務は、従業員数が250人未満の企業または組織には適用されません。ただし、当該企業または組織が行う処理がデータ主体の権利および自由に対するリスクをもたらす可能性が高い場合、処理が偶発的でない場合、または処理に特別なカテゴリーのデータまたは犯罪歴や違法行為に関連する個人データが含まれる場合は除きます。
GDPRでは、処理者が各管理者に代わって行う処理活動に関して実施したデータ保護影響評価（DPIA）の詳細を、処理者側が記録に含めることを義務付けていません。DPIAは、プロジェクトのデータ保護リスクを特定し、最小限に抑えるためのプロセスです。特定の種類の処理が自然人の権利と自由に高いリスクをもたらす可能性がある場合、管理者はDPIAを実施する責任があります。処理者は管理者によるDPIAの実施を支援することはできますが、処理活動の記録にそれを文書化する必要はありません。したがって、正解はDです。参考：
GDPR第30条(2)
GDPR第35条
ICO、ドキュメント1
ICO、データ保護影響評価1

最新問題**: 101**
第 29 条作業部会は、GDPR が 「フォーラム ショッピング」を禁止していることを強調していますが、企業が何を行うと 「フォーラム ショッピング」が発生しますか?
A. ビジネス上の懸念に最も共感してくれるデータ保護責任者を選択します。

B. 最も柔軟な慣行を持つ加盟国における主要事業所を指定します。
C. 侵害判決に対する控訴を複数の EU 機関に同時に提出します。
D. プライバシー保護の品質ではなくコストに基づいてサードパーティのプロセッサを選択します。
Answer: (解答を表示する**)**
GDPRは、EU全体のデータ保護規則を調和させ、それらの規則の一貫性と有効性を確保することを目的としています。しかし、GDPRは、加盟国間の国内法、文化、慣行の違いにより、法律の解釈と適用に若干の差異が生じる可能性があることも認識しています。そのため、GDPRは管理者または処理者の「主たる事業所」という概念を導入しています。これは、EU内で個人データの処理の目的と手段に関する決定が行われる場所です1。主たる事業所は、管理者または処理者の越境処理活動の主導機関となる国の監督機関、および紛争や苦情が発生した場合に適用される国の法律を決定します2。各国の監督機関、欧州データ保護監督機関、および欧州委員会の代表者で構成される諮問機関である第29条作業部会は、GDPRに基づく管理者または処理者の主たる事業所の特定方法に関するガイドラインを発行しています3。このガイドラインでは、主たる事業所は、処理活動の実態と、それらの活動に対する管理権限の有効かつ現実的な行使を反映しなければならないことを強調しています。ガイドラインはまた、「フォーラム・ショッピング」の慣行についても警告を発しています。これは、管理者または処理者が、意思決定やデータ処理の実際の所在地に関わらず、データ保護制度が最も柔軟または緩やかな加盟国に主たる拠点を指定する行為です。ガイドラインでは、このような慣行はGDPRで禁止されており、監督当局は管理者または処理者が主たる拠点を決定する際に用いる基準を綿密に監視・検証すると規定しています。監督当局は、主たる拠点が事実関係と一致していないと判断した場合、指定に異議を申し立て、関連する是正措置を適用することができます4。参考文献：GDPR第1条第4項(16) - 定義 - 一般データ保護規則（GDPR）
2 GDPR第56条～58条 - 協力と一貫性 - 一般データ保護規則（GDPR）3 ガイドライン
GDPR の地域的適用範囲に関する欧州データ保護会議規則 3/2018（第3 条）4 同上、14 ～ 15 ページ。
参考: https://gdprinformer.com/gdpr-articles/forum-shopping-illegal-gdpr

最新問題**: 102**
GDPR によれば、仮名個人データはどのように定義されますか?
A. データ主体を特定できなくなるような方法で匿名化されたデータ。
B. 別途保存されている追加情報を使用しなければ、特定のデータ主体に帰属できなくなったデータ。
C. 特定のデータ主体に帰属できなくなり、データを再識別する可能性もなくなったデータ。
D. 暗号化されているか、その他の技術的保護手段の対象となるデータ。
Answer: B (メーッセージを残す**)**

最新問題**: 103**
欧州連合 (EU) 加盟国で個人データを収集する場合、企業がデータ主体以外のソースから個人データを収集するには、何をする必要がありますか?
A. 対象者に収集について通知する
B. データに関する公的な通知を提供する
C. ソースのセキュリティに合わせてセキュリティをアップグレードします
D. 適切な時間内にデータを更新する
Answer: A (メーッセージを残す**)**

GDPR の第 14 条によれば、管理者がデータ主体以外の情報源から個人データを収集する場合、管理者はデータ主体に対して、管理者の ID および連絡先の詳細、処理の目的および法的根拠、関係する個人データのカテゴリ、個人データの受信者または受信者のカテゴリ、およびデータ主体の権利などの特定の情報を提供しなければなりません。
これらの情報は、個人データの取得後、合理的な期間内、遅くとも1ヶ月以内、またはデータ主体との最初の連絡時、もしくは他の受領者にデータを開示する前に提供されなければなりません。この規定の目的は、個人データの公正かつ透明な処理を確保し、データ主体の情報開示を受ける権利を尊重することです。参考文献：
* GDPR 第 14 条では、データ主体から個人データが取得されていない場合に提供される情報が規定されています。
* GDPR 第 14 条の要件と例外を説明する ICO ガイダンス。
* GDPR の第 14 条の適用に関する詳細なガイダンスを提供する EDPB ガイドライン。

最新問題: **104**
GDPR によれば、写真の処理はどのような場合に特別なカテゴリの個人データの処理とみなされるのでしょうか?
A. 自然人に関する情報を公的にアクセス可能なメディアに公開する目的で処理される場合。
B. 科学的または歴史的研究プロジェクトを進める目的で処理される場合。
C. 自然人を一意に識別または認証する目的で処理される場合。
D. 法律を遵守する目的で処理される場合。
Answer: C (メーッセージを残す)
参照 :https://www.privacy-regulation.eu/en/recital-51-GDPR.htm

最新問題: **105**
データ主体がダイレクトマーケティング活動をオプトアウトした後、管理者は何をすべきでしょうか?
A. 例外なく、データ主体に関連するすべての個人データを安全に削除します。
B. 不当な遅延なく、データ主体に対して実行されるアクションに関する情報を提供します。
C. データ主体の個人データを削除し、今後は処理しないことを第三者の受信者に通知するための合理的な措置を講じます。
D. 関連する種類の通信について、データ主体に関連する個人データの処理を控えます。
Answer: (解答を表示する)

最新問題: **106**
シナリオ
次の質問に答えるには、以下を使用してください。
アンナとフランクは二人ともグランチェスター大学で働いています。アンナはデータ保護を担当する弁護士で、フランクは工学部の講師です。大学では様々な種類の記録を保管しています。
学生記録には、氏名、学生番号、自宅住所、大学入学前の情報、大学の出席および成績記録、特別な教育ニーズの詳細、財務情報が含まれます。
自伝的資料 カリキュラム、専門家の連絡先ファイル、学生の評価、その他の関連する教育ファイルなど）を含むスタッフの記録。
卒業生記録には、出生地、生年、入学日、学位授与日などが記載されています。これらの記録は、グランチェスターの卒業生ポータルに登録した卒業生が閲覧できます。教育省の記録には、特定の人口統計グループ（第一世代の学生など）の平均的な進路予測が示されています。これらの記録には、氏名や身分証明書番号は含まれていません。
大学はセキュリティ ポリシーに従い、転送中および保存中のすべての個人データ記録を暗号化します。

フランクは、教育の質を向上させるため、工学部の学生の成績が教育省の期待値とどの程度一致しているかを調査したいと考えています。彼はアンナのデータ保護に関する研修コースを受講しており、目標達成に必要な範囲を超えて個人データを使用するべきではないことを理解しています。そこで、学生の過去の出身校、当初の成績、現在の成績、初めて進学した大学など、一部のデータのみをエクスポートするプログラムを作成しました。記録は個々の学生レベルで保管したいと考えています。アンナの研修を踏まえ、フランクは学生番号をアルゴリズムにかけ、異なる参照番号に変換します。各記録を継続的に更新できるよう、毎回同じアルゴリズムを使用します。
アンナのタスクの 1 つは、GDPR の要件に従って処理アクティビティの記録を完了することです。
GDPRの規定に従い、アンナからのメールリマインダーを受け取った後、フランクはアンナにパフォーマンスデータベースについて知らせます。
アンはフランクに、個人データを最小限に抑えるだけでなく、大学は既存データの新たな利用が許容されるかどうかを確認する必要があると説明した。また、GDPRの下では、データ処理を実施する前にリスク分析を実施する必要があるのではないかとも考えている。アンナは追加調査を行った後、フランクとこの件についてさらに話し合う予定だ。
フランクは空き時間に分析作業を行いたいと考え、データを自宅のノートパソコン（暗号化されていない）に転送しました。ところが、大学にノートパソコンを持っていく途中、電車の中で紛失してしまいます。その日、フランクは互換性のある処理について話し合うため、アンナと面会する必要がありました。セキュリティインシデントを報告する必要があるため、同時にアンナにもノートパソコンの紛失について伝えることにしました。
アンナは、この状況ではリスク分析は必要ないと考えるでしょうか?
A. データ対象者はフランクの現在の生徒ではない
B. 処理はデータ主体の権利に悪影響を及ぼさない
C. データ主体は、当初の処理に対して明確な同意を与えた
D. フランクが処理に使用しているアルゴリズムは技術的に健全である
Answer: C (メーッセージを残す**)**

最新問題**: 107**
多くの企業は、従業員の顔写真を建物入場口に印刷し、警備員が従業員を識別できるようにしています。GDPRでは顔画像が生体認証データに該当する可能性があるにもかかわらず、このような行為が認められているのはなぜでしょうか？
A. データ主体の一意の識別を確認するために生体認証データを使用すると、免除の恩恵を受けることができるためです。
B. 写真は、 特定の技術的処理」を経た場合にのみ生体認証データとして認められるためです。
C. 従業員は雇用主による写真撮影に同意した時点で、明示的に同意したものとみなされるためです。
D. 写真付き身分証明書は、 重大な公共の利益のために必要な」物理的なセキュリティ対策であるためです。
Answer: (解答を表示する**)**
参考 https://ess.csa.canon.com/rs/206-CLL-191/images/IAPP-Top-10-Operational-Impacts-of- GDPR.pdf?TC=DM&CN=CSA_OMNIA_Partners&CS=CSA&CR=T1_Gov%20GenNonProfit (11)

最新問題: **108**
欧州人権裁判所 (ECHR) と欧州連合司法裁判所 (CJEU) の役割と機能に関する重要な違いは何ですか?
A. CJEU は国内裁判所による人権判決に対する控訴を審理できますが、ECHR は審理できません。
B. ECHR は基本的権利としてのプライバシーに関する問題について判決を下すことができますが、CJEU はそれができません。
C. CJEU は各国政府に EU 法を実施し尊重するよう強制できますが、ECHR はそれができません。
D. ECHR は人権法を実施しない政府に対して人権法を強制執行できますが、CJEU はそれができません。
Answer: C (メーッセージを残す**)**

最新問題: **109**
A German data subject was the victim of an embarrassing prank 20 years ago. A newspaper website published an article about the prank at the time, and the article is still available on the newspaper's website. Unfortunately, the prank is the top search result when a user searches on the victim's name. The data subject requests that SearchCo delist this result. SearchCo agrees, and instructs its technology team to avoid scanning or indexing the article. What else must SearchCo do?
A. Identify other controllers who are processing the same information and inform them of the delisting request.
B. Notify the newspaper that its article it is delisting the article.
C. Prevent the article from being listed in search results no matter what search terms are entered into the search engine.
D. Fully erase the URL to the content, as opposed to delist which is mainly based on data subject's name.
Answer: B (メーッセージを残す**)**

最新問題: **110**
シナリオ
次の質問に答えるには、以下を使用してください。
Building Block Inc.はシカゴに本社を置き、米国、アジア、ヨーロッパ（ドイツ、イタリア、フランス、ポルトガルを含む）にオフィスを構える多国籍企業です。昨年、同社はフィッシング攻撃の被害に遭い、大規模なデータ漏洩が発生しました。取締役会は、ゼネラルマネージャー、プライバシーオフィス、情報セキュリティチームと連携し、追加のセキュリティ対策を講じることを決議しました。これには、トレーニングによる意識向上プログラム、サイバーセキュリティ監査、そしてSecurityScanと呼ばれる新しいソフトウェアツールの導入が含まれます。SecurityScanは、従業員のコンピュータをスキャンし、ベンダーによるサポートが終了してセキュリティアップデートが提供されていないソフトウェアがないか確認します。このソフトウェアは、従業員のコンピュータの監視など、他の機能も備えています。
これらの対策は従業員に影響を及ぼす可能性があるため、Building Block のプライバシー オフィスは、情報セキュリティを強化し、将来のデータ侵害を防止するための一連の取り組みを実施することを通知する一般通知を全従業員に発行することを決定しました。
これらの対策を実施した後、サーバーのパフォーマンスが低下しました。ゼネラルマネージャーは、セキュリティチームに対し、SecurityScanを使用して従業員のコンピュータのアクティビティと位置情報を監視する方法を指示しました。
これらの活動の中で、情報セキュリティチームは、イタリア出身の従業員が映画のビデオライブラリに毎日接続していること、またドイツ出身の従業員が許可なくリモートワークを行っていることを発見しました。セキュリティチームはこれらのインシデントをプライバシーオフィスとゼネラルマネージャーに報告しました。報告書の中で、チームはイタリア出身の従業員がサーバーのパフォーマンス低下の原因であると結論付けました。

これらの違反行為の重大性を考慮し、同社のセキュリティおよびプライバシーポリシーでは、従業員が会社のコンピュータにソフトウェアをインストールしたり、許可なくリモートワークしたりすることを禁止しているため、同社は両従業員に懲戒処分を適用することを決定しました。
監視の目的、データの潜在的な用途、プライバシー権について従業員に通知することに加えて、セキュリティ対策を実施する前に、Building Block は従業員にどのような情報を提供するべきでしたか?
A. 雇用契約書に規定されている内容に関する情報。
B. 従業員が質問がある場合に連絡すべき相手に関する情報。
C. 同意を与えることが従業員にどのような影響を与えるかについての情報。
D. 対策が会社にとってどのように最善の利益となるかについての情報。
Answer: B (メーッセージを残す**)**
GDPR によれば、データ主体から個人データを収集する場合、管理者はデータ主体に対して、管理者の ID および連絡先、データ保護責任者の連絡先、処理の目的および法的根拠、個人データの受領者または受領者の区分、データ主体の権利、および公正かつ透明な処理を確保するために必要なその他の情報などの特定の情報を提供しなければなりません1。この情報は、明確で平易な言葉を使用して、簡潔で透明性があり、理解しやすく、簡単にアクセスできる形式で提供されなければなりません2。したがって、Building Block は、セキュリティ対策を実施する前に、情報通知の一部として、データ保護責任者やプライバシー オフィスなど、監視に関する質問がある場合に連絡できる連絡先についての情報を従業員に提供すべきでした。これにより、従業員は、個人データの処理へのアクセス、修正、消去、制限、または異議申し立ての権利、あるいは監督機関に苦情を申し立てる権利などの権利を行使できるようになります3。参照: 1 Art. 13 GDPR - データ主体から個人データを収集する場合に提供される情報 - 一般データ保護規則 (GDPR)2 条。12 GDPR - データ主体の権利を行使するための透明な情報、コミュニケーション、方法 - 一般データ保護規則 (GDPR)3 条。15-22 GDPR - データ主体の権利 - 一般データ保護規則 (GDPR)。

最新問題**: 111**
GDPR の第 30 条に基づき、管理者は以下を除くすべての記録を保持することが義務付けられています。
A. 開示の有無にかかわらず、個人データ漏洩事件。
B. 実施されたデータ インベントリまたはデータ マッピング演習。
C. 個人データが開示された受信者のカテゴリ。
D. 個人データのカテゴリの消去および削除の保持期間。
Answer: A (メーッセージを残す**)**
GDPR第30条は、管理者と処理者に対し、処理活動の記録を保持することを義務付けています。記録には、処理の目的、個人データのカテゴリー、データの受信者、保存期間、セキュリティ対策などの情報が含まれます12。しかし、第30条は、管理者に対し、個人データ漏洩のインシデントについて、開示の有無にかかわらず記録を保持することを義務付けていません。これは、第33条および第34条に基づく別の義務であり、これらの条項では、管理者に対し、個人データ漏洩が自然人の権利と自由にリスクをもたらす可能性が低い場合を除き、監督機関およびデータ主体に個人データ漏洩を通知することを義務付けています34。参考文献 :1 :GDPR第30条 2：英国GDPR第30条に基づき文書化する必要があるものは何ですか？ | ICO 3 :GDPR第33条 4 :GDPR第34条 解説：
参考 :https://medium.com/golden-data/what-records-must-controllers-and-processors-keep-to-comply- with-eu-data-protection-law-3e8bac177695

最新問題**: 112**

A data controller appoints a data protection officer. Which of the following conditions would NOT result in an infringement of Articles 37 to 39 of the GDPR?
A. If the data protection officer receives instructions from the data controller.
B. If the data protection officer lacks ISO 27001 auditor certification.
C. If the data protection officer is provided by the data processor.
D. If the data protection officer also manages the marketing budget.
Answer: A (メーッセージを残す**)**

最新問題**: 113**
シナリオ
次の質問に答えるには、以下を使用してください。
Zandelay Fashion（以下Ƶandelay」）は、アイルランドのダブリンに本社を置き、約650人の従業員を擁する、国際的なオンライン衣料品小売業者です。マーティンは最近任命されたデータ保護責任者であり、一般データ保護規則 ⒼDPR）およびその他のプライバシー法の遵守を監督しています。
同社は、子供を含むあらゆる年齢層を対象に、男性用と女性用の衣料品ラインを提供しています。その過程で、顧客の嗜好やクレジットカード番号や銀行口座番号といった機密性の高い金融情報など、大量の顧客情報を処理しています。
収益成長を積極的に図るため、CEOのジェリーはマーティンに対し、顧客の購入履歴を分析し、プロファイリングに重点を置いた新しいモバイルアプリとロイヤルティプログラムを導入することを伝えました。マーティンはCEOに対し、(a) こうした活動に伴う潜在的なリスクを考慮すると、ザンデレイ社はこの新しい取り組みとそのプライバシーへの影響を評価するためにデータ保護影響評価を実施する必要があること、(b) この評価結果から、適切な保護措置を講じない場合に高いリスクが生じる可能性があることを示唆しました。ザンデレイ社は、アプリとロイヤルティプログラムを導入する前に、アイルランドのデータ保護コミッショナーとの事前協議を行う必要があるかもしれません。
ジェリーはマーティンに対し、監督当局と直接交渉し、ザンデレイの事業計画と関連する処理活動の詳細を開示しなければならない可能性について不満を述べている。
事前協議の際に、Zandelay は監督当局に何を提供する必要がありますか?
A. 意図した処理の複雑さの評価。
B. 意図される処理の目的と手段の説明。
C. 顧客が意図したプロファイリング活動に明示的に同意したことを示す記録。
D. Martin の専門的な資質とデータ保護法に関する専門知識を証明する証明書。
Answer: B (メーッセージを残す**)**
GDPR第36条によれば、管理者がデータ主体の権利と自由に高いリスクをもたらす個人データを処理しようとする場合、かつ、第35条に基づくデータ保護影響評価において管理者によるリスク軽減が不可能であると判断された場合、管理者は処理前に監督機関に相談しなければなりません。この事前相談の目的は、処理がGDPRに準拠しているかどうか、また準拠を確保するためにどのような措置を講じることができるかについて、監督機関から助言を求めることです。事前相談において、管理者は監督機関に以下の情報を提供しなければなりません。
* 特に企業グループ内での処理に関する、処理に関与する管理者、共同管理者および処理者のそれぞれの責任。
* 意図される処理の目的および手段
* GDPRに従ってデータ主体の権利と自由を保護するために提供される措置と保護手段。
* データ保護担当者の連絡先（該当する場合）

* 第35条に規定されるデータ保護影響評価。
* 監督当局から要求されるその他の情報。
したがって、正解はBです。意図された処理の目的と手段の説明です。この情報は、監督機関が処理の性質と範囲を理解し、GDPRへの準拠を評価するために不可欠です。その他の選択肢は、第36条では必須ではありませんが、設計によるデータ保護およびデフォルトによるデータ保護の原則（A）、処理の合法性、データ保護責任者の指定（D）など、GDPRの他の側面に関連する可能性があります。
参考文献：
* 監督当局との事前協議を規定する GDPR 第 36 条。
* 事前協議のプロセスと要件を説明する ICO ガイダンス。
* 事前協議の基準と手順に関する詳細なガイダンスを提供する EDPB ガイドライン。

最新問題: **114**
「不当な遅延なく」という規定が遵守されていると仮定した場合、データアクセス要求に応じる期限はどれくらいですか?
A. 受領後40日以内
B. 受領後40日以内。さらに40日まで延長可能
C. 受領後1ヶ月以内。さらに1ヶ月まで延長可能。
D. 受領後1ヶ月以内。さらに2ヶ月延長される場合があります。
Answer: D (メーッセージを残す)
GDPRによると、データ管理者はデータアクセス要求（SARとも呼ばれる）に対し、遅滞なく、いかなる場合でも要求受領後1ヶ月以内に回答しなければなりません。要求が複雑な場合、または管理者が同一人物から複数の要求を受け取った場合、この期限はさらに2ヶ月延長されることがあります。ただし、管理者は要求受領後1ヶ月以内に当該個人に通知し、延長が必要な理由を説明する必要があります。期限は、要求受領日の翌日（営業日かどうかは関係ありません）から翌月の該当暦日まで計算されます。該当暦日がない場合、期限は翌月末となります。期限が週末または祝日に当たる場合は、翌営業日に回答する必要があります。参考：
GDPR第12条(3)
ICO、アクセス権1
ICO、データ保護権の要求に対する回答期限2

最新問題: **115**
GDPR に基づいてデータ主体に明示的に付与される権利ではないものはどれですか?
A. 管理者が保有する個人データへのアクセスを要求する権利。
B. 管理者が保有するデータの削除を要求する権利。
C. 第三者への個人データの販売を拒否する権利。
D. 特定のシナリオ下で個人データの処理の制限を要求する権利。
Answer: C (メーッセージを残す)
GDPRは個人データの販売について具体的に規定していないため、これはGDPRの下でデータ主体に明示的に付与された権利ではありません。ただし、GDPRでは、契約や法的義務など、他の法的根拠に基づかない個人データの処理については、データ主体が同意を与えることを義務付けています1。したがって、データ主体はいつでも同意を撤回する権利を有し、管理者は同意を得る前にこの権利についてデータ主体に通知しなければなりません2。その他の選択肢は、GDPRの下でデータ主体に明示的に付与された権利であり、規則の第3章に記載されています3。参考：
無料のCIPP/E学習ガイド、23ページ、セクション3.1

CIPP/E認証、18ページ、セクション3.1
2023年版CIPP/E究極学習ガイド、16ページ、セクション3.1
GDPRデータ主体の権利 - 8つの基本的権利と追加的権利、第4項 データ主体の権利 - 一般データ保護規則（GDPR）、第7条 データ主体の権利 - 一般データ保護規則（GDPR）、第3章

最新問題: **116**
シナリオ
次の質問に答えるには、以下を使用してください。
ProStorageは、オランダに本社を置く多国籍クラウドストレージプロバイダーです。CEOのルース・ブラウン氏は、成長のために2本柱の戦略を立てました。1) ProStorageの顧客ベースを世界中に拡大し、2) 効果的なチームを効率的に採用してProStorageの営業部隊を増強することです。この戦略の実行は、ルースの健康状態により、最近、労働時間が制限され、潜在顧客に会うために出張することも困難になったため、複雑になっています。ProStorageの人事部とルースの首席スタッフは現在協力して、彼女のスケジュールを管理し、彼女がすべての医療予約を確実に受けられるようにしています。後者は、ルースが前回インドを旅行した際に健康上の緊急事態に見舞われ、ニューデリーで入院して以来、特に重要になっています。ルースの家族と連絡が取れなかったため、病院はProStorageに連絡し、首席スタッフと連絡を取ることができました。首席スタッフは、人事部長のメアリーと連携していました。ルースが ProStorage を始めたときに出したリクエストに応じて、医師に情報を提供しました。より多くの営業担当者を雇うというルースの戦略目標をサポートするために、人事チームは、新しい従業員の募集、面接、雇用、オンボーディングを効率的に行うためのプロセスの改善に注力しています。これを支援するため、メアリーはドイツを拠点とする HRYourWay とオーストラリアを拠点とする InstaHR という 2 つのベンダーを特定しました。彼女は、ルースと協力して最終決定を下せるよう、両方のベンダーに ProStorage のベンダーリスクレビュープロセスを実行してもらうことにしました。レビュープロセスの一部として、ProStorage のプライバシープログラムの維持 (コントローラー BCR の維持とベンダーリスク評価の実施を含む) を担当しているジャッキーが両方のベンダーをレビューしましたが、移管影響評価は InstaHR についてのみ完了しました。彼女のレビュー後、どちらもより確立されたプライバシープログラムを誇り、サードパーティの認証を提供していましたが、HRYourWay はデータ保護操作が最小限の小規模ベンダーでした。
そこで彼女はInstaHRを勧めました。
ProStorageのマーケティングチームは、市場シェア拡大が必要な業界に注力することで、同社の戦略目標の達成にも取り組みました。この取り組みを支援するため、チームは金融業界の顧客と深い関係を持つ米国企業であるUpFinanceをパートナーとして選定しました。ProStorageのデューデリジェンスプロセスにおいて、プライバシーチームのジャッキーは、移転影響評価において、UpFinanceがエンドツーエンドの暗号化（暗号鍵は顧客が保有）を含む複数のデータ保護対策を実施していることを指摘しました。
注目すべきことに、UpFinanceは創業7年間、政府からの要請を一度も受けていません。それでもジャッキーは、UpFinanceが代理で処理する個人データについて政府からの要請を受けた場合、当該データを開示する前にProStorageに通知することを契約に盛り込むことを推奨しました。
ProStorage は、ルースの医療情報を病院に転送するために、どのような転送メカニズムに頼ったと考えられますか?
A. ルースの暗黙の同意。
B. ルツの重大な利益を守る
C. ルースとの契約の履行。
D. ルースからの法的責任から保護します。
Answer: B (メーッセージを残す**)**

GDPR第49条によれば、個人データの第三国または国際機関への移転は、十分性認定または標準契約条項や拘束的企業準則などの適切な保護措置がない場合でも、同条に列挙されている例外のいずれかが適用される場合にのみ行うことができます1。例外の一つは、データ主体が身体的または法的に同意できない場合に、データ主体または他の人の重大な利益を保護するために移転が必要な場合です1。この例外は、医療上の緊急事態など、移転がデータ主体の生命または健康にとって不可欠である緊急事態のみを対象とすることを目的としています2。
このシナリオでは、ProStorage社は、ルースさんの医療情報をインドの病院に転送するために、この例外規定に依拠した可能性が高いと考えられます。ルースさんはインドの病院で緊急医療を受け、入院しました。ルースさんは危篤状態にあり、緊急の医療処置を必要としていたため、この転送はルースさんの重大な利益を保護するために必要でした。また、ルースさんは意識不明または無能力状態であったため、身体的または法的に同意を与えることができませんでした。したがって、選択肢Bが正解です。
選択肢Aは誤りです。ルースの黙示的な同意は、GDPRの下では有効な移転メカニズムとはみなされません。第三国または国際機関への個人データの移転については、明示的、情報に基づいた、具体的、かつ自由意志による同意が必要です1。ルースは、自身の医療情報を病院に移転することについて、明示的な同意を与えておらず、そのことについて通知も質問もされていませんでした。さらに、データ主体が医療上の緊急事態など、苦痛や依存の状況にある場合、同意は自由意志によるものとはみなされないため、移転メカニズムとして依拠することはできません2。
選択肢Cは誤りです。なぜなら、ルースとの契約の履行は、GDPRの下では有効な移転手段ではないからです。データ主体との契約に基づく第三国または国際機関への個人データの移転は、当該契約の履行、またはデータ主体の要請に基づく契約前措置の実施に必要な場合にのみ許可されます1。このシナリオでは、ProStorageとルースの間に、ルースの医療情報を病院に移転することを義務付けたり正当化したりする契約は存在しません。この移転は、ルースとProStorageとの雇用契約の履行にも、ルースが行う契約前措置にも必要ありません。
選択肢Dは誤りです。Ruthからの法的責任に対する保護は、GDPRの下では有効な移転メカニズムではないためです。法的請求または防御を理由とする第三国または国際機関への個人データの移転は、法的請求の確立、行使、または防御に必要な場合にのみ許可されます1。このシナリオでは、Ruthの医療情報を病院に移転することに関連する法的請求または防御はありません。この移転は、ProStorageまたはRuthによる、またはProStorageまたはRuthに対する法的請求の確立、行使、または防御に必要ではありません。
参照：
特定の状況における例外
規則2016/679に基づく第49条の例外に関するガイドライン2/2018

最新問題**: 117**
2016 年のガイダンスでは、英国の情報コミッショナー事務局 (ICO) は、データ主体に何を提供するために 階層化された通知」を使用することの重要性を再確認しましたか?
A. ウェブサイト上での Cookie の使用をオプトアウトした場合の結果を説明するプライバシー通知。
B. 書面による同意が求められる加盟国において、書面による同意を提供するための効率的な手段。
C. 個人データを第三者に転送する際に適用されるセキュリティ対策の説明。
D. 簡単な情報が記載されたプライバシー通知で、詳細情報へのアクセスも提供します。
Answer: D (メーッセージを残す**)**

最新問題**: 118**
シナリオ

次の質問に答えるには、以下を使用してください。
イタリアに拠点を置くBHealthyは、日焼け止めを中心とした新しい自然派製品ラインの発売準備を整えています。製品発売前の最後のステップとして、BHealthyはヨーロッパ全域で新しい日焼け止めラインをどの程度広く販売するかを決定するための調査を実施します。この調査にあたり、BHealthyは自然派製品の価格設定を専門とするNatural Insightと提携しました。BHealthyは、既存の顧客情報（氏名 所在地、過去の購入履歴）をNatural Insightと共有することを決定しました。Natural Insightはこの情報を用いてアルゴリズムをトレーニングし、BHealthyが新しい日焼け止めを販売する価格帯を決定する予定です。
BHealthyは顧客リストの共有に先立ち、Natural Insightのセキュリティ対策をレビューし、同社が連絡先情報を保護するための十分なセキュリティ対策を講じていると結論付けました。さらに、BHealthyとNatural Insightとのデータ処理契約条件では、技術的および組織的な対策の継続的な実施が義務付けられています。また、契約には、BHealthyから提供されたデータをサービス提供以外の目的で使用すること、つまりNatural Insightの機械学習アルゴリズムの継続的な改善のためにデータを使用することが制限されていることも明記されています。
Natural Insight がアルゴリズムの改善のために BHealthy のデータを利用する場合、それがデータ処理者の活動とみなされるのはどのような場合ですか?
A. Natural Insight が BHealthy のデータを使用して、BHealthy の価格ポイント予測を改善する場合のみ。
B. Natural Insight が BHealthy から、アルゴリズムの改善のためにデータを使用するという明示的な契約上の指示を受けた場合。
C. Natural Insight が製品改善活動において BHealthy の顧客情報を使用することについて全責任を負うことに同意する場合。
D. Natural Insight が、BHealthy の顧客に製品改善活動のために顧客情報を利用する計画を通知することにより、透明性の要件を満たしている場合。
Answer: B (メーッセージを残す**)**
一般データ保護規則（GDPR）によれば、データ処理者とは、データ管理者に代わって個人データを処理する自然人、法人、代理店、公的機関、またはその他の団体を指します。データ管理者とは、個人データの処理の目的と手段を単独または共同で決定する自然人、法人、代理店、公的機関、またはその他の団体を指します。GDPRは、データ管理者とデータ処理者の両方に特定の義務と責任を課し、処理の対象、期間、性質、目的、およびデータ管理者の義務と権利を規定した書面による契約またはその他の法的行為を締結することを義務付けています。
このシナリオでは、BHealthyがデータ管理者であり、顧客情報を収集し、Natural Insightと共有する目的と手段を決定します。Natural Insightはデータ処理者であり、BHealthyの新しい日焼け止めの価格を決定する目的でBHealthyに代わって顧客情報を処理し、BHealthyの目的や指示に沿わない可能性があります。これは、データ処理者は、EUまたは加盟国の法律で義務付けられている場合を除き、データ管理者からの文書化された指示に基づいてのみ個人データを処理する必要があるため、データ処理契約およびGDPRに違反する可能性があります（GDPR第28条(3)(a)）。
したがって、Natural Insight がアルゴリズムの改善のために BHealthy のデータを使用することがデータ処理者の活動とみなされる唯一のケースは、Natural Insight が BHealthy から、アルゴリズムの改善のためにデータを使用するという明示的な契約上の指示を受けた場合です。これは、BHealthy が Natural Insight がその特定の目的のためにデータを処理することに同意し、許可し、Natural Insight が BHealthy の指示に従って行動していることを意味します。この場合、Natural Insight は依然としてデータ処理契約と GDPR に拘束され、データのセキュリティの確保、別の処理者を雇用するための条件の尊重、データ管理者による GDPR 遵守の確保の支援、サービス終了後のデータの削除またはデータ管理者への返却など、データ処理者のその他の義務と要件を遵守する必要があります。
その他の選択肢は、データ管理者の指示や同意を必要としないため、データ処理者の活動として認められません。Natural InsightがBHealthyのデータをBHealthyの価格予測の改善のみに利用している場合でも、データが収集・共有された目的とは異なる目的で、BHealthyの認識や承認なしにデータを処理している可能性があります。Natural Insightが製品改善活動におけるBHealthyの顧客

情報の使用について全責任を負うことに同意した場合でも、データ管理者の代理ではなく自社の利益のために行動しているため、データ処理契約およびGDPRに違反している可能性があります。Natural InsightがBHealthyの顧客に、製品改善活動のために顧客情報を使用する計画を通知することで透明性要件を満たしている場合でも、データ管理者の役割はデータ主体に処理活動を通知することではなく、自社の目的でデータを処理する法的根拠がない可能性があるため、データ管理者の権利と義務を侵害している可能性があります。
参照：
GDPR
データ管理者および処理者 - GDPR EU
英国GDPRは誰に適用されますか？ | ICO
GDPR ではどのような活動が処理としてカウントされますか?
データ処理とは何ですか？ - 欧州委員会

最新問題: **119**
GDPR第80条(1)に基づき、個人はプライバシーに関する集団訴訟またはクラスアクションにおいて、非営利団体を代理人として選任することができます。これらの団体は一般的に何と呼ばれていますか？
A. 市民社会組織。
B. 人権団体。
C. 法律事務所組織。
D. 憲法上の権利団体。
Answer: (解答を表示する**)**

最新問題: **120**
GDPRは、特定の違反に対してデータ管理者に課される可能性のある罰金を規定しています。以下の違反のうち、最高1,000万ユーロまたは企業の場合は前会計年度の全世界の年間売上高の2%以下）の軽微な行政罰金の対象となるのはどれですか？
A. 個人データが処理の根拠として使用される際に、データ主体がその処理に同意したことを証明できない場合。
B. データ保護が設計およびデフォルトで確実に実現されるようにするための技術的および組織的な対策を実施していない。
C. 個人情報を本来の目的に沿った方法で処理しなかった場合。
D. データ主体に対して個人データの不正確さを修正する手段を提供していない。
Answer: (解答を表示する**)**
GDPR第83条によれば、管理者および処理者、認証機関、監視機関に関する条項の違反には、最大1,000万ユーロまたは全世界の年間売上高の2%という軽微な行政罰が適用されます。これらの条項には、第8条、第11条、第25条から第39条、第42条、および第43条が含まれます。選択肢の中で、このカテゴリーに該当するのは選択肢Bのみです。これは、第25条が管理者に対し、設計段階およびデフォルト段階におけるデータ保護の実装を義務付けているためです。選択肢Aは、同意の条件を規定する第7条に関連します。選択肢Cは、個人データ処理の原則を規定する第5条に関連します。選択肢Dは、データ主体に訂正権を付与する第16条に関連します。これらの条項には、最大2,000万ユーロまたは全世界の年間売上高の4%という、より重度の行政罰が適用されます。参考文献：
* GDPR第83条
* GDPR第25条
* GDPR第7条
* GDPR第5条
* GDPR第16条

最新問題: **121**
世界人権宣言（1948 年）では、私生活および家庭生活の権利（第12 条）が他のどの権利と関連していますか?
A. 表現の自由。
B. 集会および結社の自由。
C. 差別の禁止。
D. 自らの宗教を表明する自由。
Answer: A (メーッセージを残す**)**
UDHR からの正確な抜粋（CIPP/E 第 3 版で基礎的な人権文書を扱う際に依拠した主要な情報源）:
* 第12条（プライバシーの権利）：何人も、その私生活、家族、住居、通信に対して恣意的に干渉され、又は名誉及び信用に対して攻撃を受けることはない。すべての者は、このような干渉又は攻撃に対して法律の保護を受ける権利を有する。」
* 第19条（意見及び表現の自由）：すべての者は、意見及び表現の自由を有する。この権利には、干渉を受けることなく意見を有する自由並びにあらゆる媒体を通じて、また国境を問わず、情報及び考えを求め、受け、及び伝える自由が含まれる。」これらの2つの世界人権宣言の条項は、欧州データ保護の歴史的基盤の一部として、CIPP/Eで併せて学習されます。プライバシー（第2条）は、表現の自由（第9条）とバランスが取れています。CIPP/E公式教科書（第3版）は、GDPRをこの人権の枠組みに明確に位置づけており、欧州データ保護法の起源と発展に関する導入章で世界人権宣言を取り上げています。
（CIPP/E 資料で頻繁に強調されている文脈注記：世界人権宣言では、権利のバランス（プライバシーと表現が一緒に読まれる理由）についても説明しており、第 29 条 (2) で、権利と自由を行使する際には、「他者の権利と自由に対する正当な認識と尊重を確保する目的でのみ」、法律によって制限を課すことができるとされています。）

最新問題: **122**
「不当な遅延なく」という規定が遵守されていると仮定した場合、データアクセス要求に応じる期限はどれくらいですか?
A. 受領後40日以内
B. 受領後40日以内。さらに40日まで延長可能
C. 受領後1ヶ月以内。さらに1ヶ月まで延長可能。
D. 受領後1ヶ月以内。さらに2ヶ月延長される場合があります。
Answer: (解答を表示する**)**
GDPRによれば、データ管理者はデータアクセス要求（SARとも呼ばれる）に対し、遅滞なく、いかなる場合でも要求受領後1ヶ月以内に応答しなければなりません。要求が複雑な場合、または管理者が同一人物から複数の要求を受け取った場合、この期限はさらに2ヶ月延長されることがあります。ただし、管理者は要求受領後1ヶ月以内に当該個人に通知し、延長が必要な理由を説明する必要があります。期限は、要求受領日の翌日（営業日かどうかは関係ありません）から翌月の該当暦日まで計算されます。該当暦日がない場合、期限は翌月末となります。期限が週末または祝日に当たる場合は、翌営業日に回答する必要があります。参考資料：

* GDPR第12条(3)
* ICO、アクセス権1
* ICO、データ保護権の要求に対する回答期限2
参考 :https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

最新問題**: 123**
シナリオ
次の質問に回答するには、以下を使用してください: 01
ベッドロック保険の長年の顧客であるルイスさんは、数ヶ月前に軽微な交通事故に遭いました。けが人はいませんでしたが、ルイスさんは 「アクシデンタブル」という会社から、人身傷害の賠償金回収を支援するという内容のメッセージや電話に悩まされています。保険会社が顧客のデータを第三者に販売していると聞いていたルイスさんは、「アクシデンタブル」がベッドロック保険から自分の情報を入手したに違いないと確信しています。
ルイはまた、ベッドロック社からあらゆる種類の保険を売りつけようとするマーケティング情報をますます多く受け取るようになった。
これに動揺したルイは、インターネットの価格比較サイトを調べ始めました。長年ベッドロックの忠実な顧客であったにもかかわらず、他の保険会社がベッドロックよりもはるかに安い保険料を提示していることに気づき、衝撃を受けました。ベッドロックの保険の更新時期が来たとき、彼はザントルム保険に乗り換えることにしました。
新しい保険契約を有効にするには、ルイは無事故割引、車両、運転履歴に関する情報をZantrumに提供する必要があります。GDPRに基づく自身の権利を調べた後、彼はBedrockに対し、自身の情報をZantrumに直接転送するよう依頼する書面を提出しました。また、この機会に、Bedrockに対し、マーケティング目的での個人データの使用を停止するよう要請しました。
ベッドロックはルイに無事故証明書のPDF版とXML版（拡張マークアップ言語）を提供したが、技術的に不可能であるため、ルイのデータをザントルムに直接転送することはできないと告げた。ベッドロックはまた、ルイの契約書には、ルイが自身のデータをマーケティング目的で使用することに同意するという条項が含まれていたと説明した。ベッドロックによると、ルイがこの件について考えを変えるには遅すぎるという。契約書の文言を思い出すと、法律用語が満載で非常に分かりにくかったルイは憤慨した。
その間も、ルイはアクシデンタブル -インシュアランスから迷惑電話を受け続けています。彼はアクシデンタブル -インシュアランスに手紙を書き、自分の個人情報を提供した組織の名前を尋ねました。彼はアクシデンタブル -インシュアランスが自分のデータを不法に使用していると考えており、データ保護当局に苦情を申し立てるつもりだと警告しました。手紙には、いかなる形であれ自分のデータがアクシデンタブル -インシュアランスに利用されることを望まない旨が記されていました。
アクシデンタブルからの返信は、ルイスの疑念を裏付けるものでした。アクシデンタブルはベッドロック -インシュアランスの完全子会社であり、ルイスが事故の保険金請求を提出した直後にベッドロックからルイスの事故に関する情報を受け取りました。アクシデンタブルは、ルイスの契約書にビジネス目的でベッドロックの関連会社と情報を共有することに同意する条項が含まれていたため、GDPR違反はないとルイスに保証しました。
ルイはベッドロック社による扱いに嫌悪感を抱き、自分の情報をすべてコンピューター システムから消去するよう要求する手紙をベッドロック社に送りました。
ダイレクトマーケティング目的での個人データの使用に関する GDPR の立場に基づくと、データ主体としてのルイの権利について正しいのは次のうちどれですか。
A. ルイは以前同意したため、自分のデータの使用に異議を申し立てる権利はありません。

B. Louis は、法的請求を実行する目的で Bedrock によってデータが必要な場合を除き、データの使用に異議を申し立てる権利を有します。
C. Bedrock が処理の正当な根拠を証明できる場合、Louis にはデータの使用に異議を申し立てる権利はありません。
D. Louis はいつでも自分のデータの使用に異議を申し立てる権利を有し、Bedrock は使用停止の要求を尊重しなければなりません。
Answer: (解答を表示する**)**

最新問題**: 124**
GDPR では、国境を越えた移転に関する適切性の決定に関して正しいのは次のうちどれですか。
A. 欧州委員会は、個々の企業に対して適正性決定を下すことができます。
B. 欧州委員会は、既存の適格性決定を採用、廃止、または修正することができます。
C. EU 加盟国には、欧州委員会の適正性決定を承認または拒否する権限が与えられています。
D. 適切であるとみなされるためには、第三国は EU 一般データ保護規則を国内法に導入する必要があります。
Answer: B (メーッセージを残す**)**
GDPR第45条に基づき、欧州委員会は、第三国、第三国内の地域もしくは一つ以上の特定のセクター、または国際機関が個人データの適切な保護水準を確保しているかどうかを判断する権限を有します。これは、EUおよびEEAから当該第三国へ、追加の保護措置を必要とせずに個人データを流すことができることを意味します。適切性に関する決定は、当該第三国または第三機関の法的枠組み、執行メカニズム、公的機関によるアクセス、国際的なコミットメント、およびEUとの協力関係の評価に基づいて行われます。欧州委員会はまた、適切性に関する決定の運用状況を監視し、保護水準が確保されなくなった場合には、決定を撤回、修正、または停止することができます。欧州委員会はこれまでに、日本、カナダ、スイス、英国、EU-米国データプライバシーフレームワークなど、複数の国および機関が適切な保護を提供していると認定しています。参考文献 :GDPR第45条、非EU加盟国におけるデータ保護の適切性、適切性に関する決定 | 欧州データ保護委員会

最新問題**: 125**
GDPR のどの側面が、欧州連合全体でのデータ保護法の一貫した実施に最も影響を与えると考えられますか?
A. 本質的にはワンストップショップの仕組みとして機能する
B. 指令ではなく規則の形をとること
C. 大規模なデータ侵害の通知を義務化する
D. データ保護責任者の任命を義務付ける
Answer: B (メーッセージを残す**)**
One of the main differences between a Regulation and a Directive in the EU law is that a Regulation is directly applicable and binding in all EU member states, without the need for national implementing measures, while a Directive sets out the objectives and principles that the member states must achieve, but leaves them the choice of form and methods to transpose it into their national laws. Therefore, by taking the form of a Regulation, the GDPR aims to harmonize and unify the data protection rules across the EU, and to ensure a consistent implementation and enforcement of the data protection laws throughout the EU. The other aspects of the GDPR listed in the question, such as the one-stop shop mechanism, the mandatory notification of large-scale data breaches, and the mandatory appointment of a data protection officer, are also important features of the GDPR, but they do not have the same impact on the consistency of the data protection laws as the form of a Regulation.

最新問題**: 126**

第三国および国際機関との関係において、データ保護法の施行のための国際協力メカニズムを開発するために、監督当局とともに適切な措置を講じるべきは次のどれですか。
A. 欧州議会
B. 指定されたデータ保護責任者
C. 欧州連合理事会。
D. 欧州委員会
Answer: B (メーッセージを残す)

最新問題**: 127**
Which of the following Convention 108+ principles, as amended in 2018, is NOT consistent with a principle found in the GDPR?
A. The necessity of the bulk collection of personal data by the government.
B. The obligation of companies to declare data breaches.
C. The requirement to demonstrate compliance to a supervisory authority.
Answer: (解答を表示する)

最新問題**: 128**
透明性の原則に関連して公正な処理慣行と見なされないものは次のどれですか?
A. ウェブサイト環境で多層的なプライバシー通知を提供します。
B. CCTV 標識に、より詳細なプライバシー通知にリンクする QR コードを表示します。
C. 紙媒体の申請書に、組織のホームページへのハイパーリンクを提供します。
D. 現場からのオンライン アプリケーションで、ジャストインタイムのコンテキスト ポップアップ プライバシー通知を提供します。
Answer: C (メーッセージを残す)
透明性原則に基づき、データ管理者は、データ主体に対し、個人データの処理方法に関する明確かつ透明性のある情報を提供しなければなりません。この情報は、容易にアクセスでき、理解しやすいものでなければなりません。紙媒体の申請書に組織のホームページへのハイパーリンクを記載することは、透明性原則に照らして公正な処理慣行とはみなされません。なぜなら、処理の具体的な目的と法的根拠、データ保護に関する権利と義務、そしてデータ管理者とデータ保護担当者の連絡先について、データ主体に直接情報を提供していないからです。これらの情報は、簡潔で分かりやすく、容易にアクセスできる形式で、明確で平易な言葉を用いて、コミュニケーション手段に適した方法で提供されるべきです。紙媒体の申請書に組織のホームページへのハイパーリンクを記載することは、これらの基準を満たしておらず、インターネットにアクセスできない、またはハイパーリンクの使い方に慣れていない一部のデータ主体にとってはアクセスできない可能性があります。したがって、この選択肢は透明性原則に照らして公正な処理慣行とはみなされません。参考文献 :1234 https://ico.org.uk /for-organisations/direct-marketing-and-privacy-and-electronic-communications/guidance-for-the-use-of- personal-data-in-political-campaigning-1/lawful-fair-and-transparent-processing/ https://ico.org.uk/for- organisations/direct-marketing-and-privacy-and-electronic-communications/guidance-for-the-use-of-personal- data-in-political-campaigning-1/lawful-fair-and-transparent-processing/

最新問題**: 129**
シナリオ
次の質問に答えるには、以下を使用してください。
ジョーは、DNA鑑定サービスを提供するカナダ企業Who-RUの新しいプライバシーマネージャーです。本社はモントリオールにあり、従業員全員がそこに勤務しています。同社はカナダ人のみにサービスを提供しています。ウェブサイトは英語とフランス語で提

供され、カナダの通貨のみを受け付け、カナダ国外からのインターネットトラフィックをブロックしています（ただし、この対策でカナダ国外からのトラフィックをすべてブロックできるわけではありません）。また、DNAレポートをカナダ国外に送付するよう要求する注文は処理せず、カナダ国外の返送先住所が記載されている注文は返品されます。
Who-RU の社長であるボブ氏は、EU でこの製品に対する関心が非常に高いと考えており、同社は顧客基盤を拡大するためのさまざまな計画を検討している。
最初の計画は、共同でWe-Track-Uと名付けられ、アプリを用いて既存のカナダの顧客基盤に関する情報を収集します。この拡張により、カナダの顧客は海外旅行中にアプリを使用できるようになります。ボブは、このアプリを用いて位置情報の収集を行うことを提案します。この計画が有望であれば、ボブはプッシュ通知とテキストメッセージを用いて既存顧客にEU版サービスの事前登録を促すことを提案します。ボブはこの作業計画をWe-Text-Uと呼んでいます。十分な事前登録数を集めた後、EU向けのコンテンツとサービスを開発する予定です。
もう1つのプランは「Customer for Life」と呼ばれる。これは、同社のアプリを通じて、DNA情報の保存や、他のアプリや医療機関との共有といった追加サービスを提供するという構想だ。同社の契約書には、顧客のDNAを無期限に保管し、新サービスの提供や顧客へのマーケティングに活用できることが明記されている。また、顧客はダイレクトマーケティングへの同意を撤回しないことに同意する、と明記されている。マーケティングディレクターのポール氏は、同社がこれらの条項を最大限に活用し、契約によって同意が無効となるため、顧客が同意を撤回しようとしても回避できると提案している。
最終計画は、EUにおけるブランドプレゼンスの構築です。同社はすでにこのプロセスに着手しており、ドイツにあるビルの命名権を購入する手続きを進めています。このビルには、Who-RUの幹部が海外旅行中に利用できるオフィススペースがいくつか設けられる予定です。このオフィスにはテクノロジーやインフラ設備は一切なく、机と椅子がいくつか置かれただけのシンプルな部屋です。
命名権契約に関する最近の出張中、ボブのノートパソコンが盗まれました。ノートパソコンには、Who-RUの顧客5,000人（全員カナダ在住）の暗号化されていないDNAレポートが保存されていました。レポートには、顧客名、生年月日、民族、人種的背景、親族名、性別、そして時折健康情報も含まれていました。
Who-RU が We-Track-U パイロット計画を採用した場合、なぜそれが GDPR の地域的適用範囲の対象となる可能性があるのでしょうか?
A. その計画は、EU 内に管理者を設立するという文脈の中で行われることになります。
B. EU 内のデータ主体に商品やサービスを提供することになります。
C. 欧州連合内で商業活動を行っています。
D. EU 内のデータ主体の行動を監視しています。
Answer: (解答を表示する**)**
GDPR によれば、規則の適用範囲は、EU 内に拠点がない管理者または処理者による、EU 内にいるデータ主体の個人データの処理に適用され、処理活動は以下に関連している場合に限ります。(a) データ主体の支払いが必要かどうかに関わらず、EU 内のそのようなデータ主体への商品またはサービスの提供、または (b) EU 内で行われる限りの行動の監視1。このシナリオでは、Who-RU は EU 内に拠点がありませんが、EU を含む海外旅行中にアプリを使用するカナダ人の顧客の位置情報を収集しています。これは、EU 内での行動の監視を構成し、したがって GDPR の適用を引き起こします。その他のオプションは正しくありません。理由は、(A) 命名権契約にはテクノロジーやインフラストラクチャが関係しないため、Who-RU は EU 内に拠点がありません。(B) Who-RU はカナダ人の顧客のみを対象とし、カナダ国外からのインターネット トラフィックをブロックしているため、EU 内のデータ主体に商品やサービスを提供していません。Who-RUはカナダ通貨のみを受け付けており、DNAレポートをカナダ国外に送付する注文は処理していないため、EU域内での商業活動には従事していません。参考文献 :1 :GDPR第3条(2)、無料CIPP/E学習ガイド、11ページ。

最新問題**: 130**

組織がランサムウェア攻撃の範囲を特定するために内部調査を実施したら、プロセスの次のステップとして適切なものは何でしょうか?
A. 侵害に関連するリスクを評価し、必要に応じて、関連する時間枠内に影響を受ける個人と規制機関に通知します。
B. 法執行機関に通知し、法律顧問に相談して、違反の影響と通知要件を理解します。
C. 関連情報が迅速に広まるよう、ソーシャル メディア プラットフォームを通じてすべての顧客と一般の人々に通知します。
D. さらなる措置を講じる前に、法執行機関が通知手順に関するガイダンスを提供するのを待ってください。
Answer: A (メーッセージを残す)
GDPR（一般データ保護規則）は、特に個人データに影響を与えるランサムウェア攻撃に対して、厳格なデータ侵害対応要件を定めています。社内調査後の適切な次のステップは、侵害に関連するリスクを評価し、必要に応じて影響を受ける関係者に通知することです。
GDPR違反対応の主な手順（第3条および第34条）
* 個人データに対するリスクを評価する
* 違反が個人の権利と自由にリスクをもたらす場合、監督機関 (DPA) に 72 時間以内に通知する必要があります。
* リスクが高い場合は、影響を受ける個人にも遅滞なく通知する必要があります。
* 回答選択肢Aが正しい理由
* リスク評価は、内部調査後の重要な第一歩です。
* 違反がリスクしきい値を満たしている場合、GDPR に基づいて当局および個人への通知が義務付けられます。
* 他の回答の選択肢が間違っている理由:
* B (まず法執行機関に通知): 法執行機関が関与する場合もありますが、GDPR では、リスク評価を実施したり個人に通知する前に法執行機関に相談することを義務付けていません。
* C（一般への即時通知）ソーシャルメディアを通じた情報公開はGDPRの要件ではありません。影響を受ける個人およびDPAには、まず正式な通知を行う必要があります。
* D（法執行機関の対応待ち）GDPRでは、通知義務を履行する前に法執行機関の対応を待つことは認められていません。管理者は72時間以内に行動を起こさなければなりません。
結論: 内部調査後の正しい次のステップは、リスクを評価し、必要に応じて、GDPR の第 33 条および第 34 条に従って、影響を受ける個人および規制機関に通知することです。

最新問題**: 131**
シナリオ
次の質問に答えるには、以下を使用してください。
TripBliss Inc.は、ここ数年で大幅な収益減少に陥っている旅行サービス会社です。新任マネージャーのオリバーは、その一因として会社のウェブサイトの老朽化が考えられます。調査を行った後、彼は新興IT企業Techivaの営業担当者と面談し、TripBliss Inc.の経営難に陥った事業のために、最先端のウェブサイトを新たにデザインしてくれることを期待します。
交渉中、Techiva の担当者は、詳細なアンケートを通じてより多くの顧客情報を収集する計画について説明しました。この情報は、顧客の好みを特定の旅行先に合わせて調整するために使用できます。
TripBliss Inc.は、年齢、収入、民族など、目標達成に最も役立つデータカテゴリーをいくつでも選択できます。オリバーはこのアイデアに満足していますが、アンケート調査では顧客からデータ収集への明示的な同意を得る必要があるため、このアプローチの成功度を測る方法も必要です。Techivaの担当者は、顧客がどのようにウェブサイトを利用しているかをより深く理解するために、新しいウェブサイトのトラフィックを分析するプログラムも実行することを提案しました。担当者は、顧客のデバイスに複数のCookieを配

置する計画を説明します。これらのCookieにより、TripBliss Inc.はIPアドレスやその他の情報を収集できます。例えば、顧客がどのサイトからアクセスしたか、TripBliss Inc.のウェブサイトで過ごした時間、どのページを訪問したかなどです。これらの情報はすべてログファイルにまとめられ、Techivaが専用のプログラムで分析します。TripBliss Inc.は、ウェブサイトの効果を評価するために、集計統計情報を受け取ります。オリバーは、これらのサービスをTechivaに積極的に依頼しています。
Techiva社は、長年のアカウントマネージャーであるレオン・サントス氏に、プロジェクトの分析部分を委託しました。通常の業務手順通り、レオン氏にはTripBliss社のウェブサイトの管理者権限が与えられ、そこから収集されたログファイルへのアクセスを許可することができます。しかし、TripBliss社にとって残念なことに、レオン氏がこの新しいプロジェクトを引き受けたのは、Techiva社への不満が最高潮に達していた時期でした。会社から不当な扱いを受けたと感じたレオンは、復讐のため、趣味でハッカーをしている友人のフレッド氏に協力を求めます。二人は協力して、フレッド氏にTechiva社のシステムに侵入させ、ログファイルをUSBメモリにコピーするという計画を立てます。
当初、レオンはUSBメモリをマスコミとデータ保護当局に送り、Techiva社を告発するつもりだったが、良心の呵責に襲われ、計画を思いとどまる。USBメモリからすべてのデータを安全に消去し、会社のアクセス制御システムを見直す必要があると上司に伝えることにした。
TripBliss Inc. が監督当局に事件を報告しないことを決定した場合、最善の防御策は何でしょうか?
A. このインシデントは、第三者の制御不能な行為によって発生しました。
B. データ主体に通知する義務が生じると、不釣り合いな労力がかかります。
C. 盗まれたデータが破壊されるため、影響を受けるデータ主体にリスクが発生する可能性は低くなります。
D. インシデントに関係するデータのカテゴリの機密性は十分に高くありませんでした。
Answer: (解答を表示する)

最新問題: **132**
GDPR の第 58 条では、欧州連合 (EU) 加盟国の監督当局の権限について次のどれが説明されていますか?
A. 調査目的でデータにアクセスする権利。
B. 加盟国内で選出された公務員の目標を遂行する裁量権。
C. 行政命令によって新しい法律を制定する権限。
D. コントローラーが法廷で有罪と判断された場合に罰則を選択する権限。
Answer: A (メーッセージを残す)

最新問題: **133**
シナリオ
次の質問に答えるには、以下を使用してください。
ジェーン・スタンは、マルタに拠点を置く企業でデータ保護責任者（DPO）として新たな役割を担っています。同社は、オンラインプラットフォームを通じて誰でも仮想通貨を売買できるサービスを提供しています。同社は顧客の個人データを、マルタ（EU）にある専用データセンターで保管・処理しています。
暗号通貨の取引を希望する人は、プラットフォーム上でオンラインアカウントを開設する必要があります。その後、マネーロンダリングの防止と適用される金融規制の遵守を目的としたKYCデューデリジェンス手続きに合格する必要があります。
欧州以外の顧客は、プラットフォーム上でアカウントを承認してもらうために、別のページの太字で書かれたチェックボックスにチェックを入れた免責事項を読んで、GDPR のすべての権利を放棄する必要もあります。

顧客も同様に、プラットフォームの利用規約に同意する必要があります。利用規約にはプライバシーポリシーのセクションも含まれており、例えば GDPRを遵守するために、サイバーセキュリティ評価者は企業とデータ処理契約を締結する必要があるか？」といった記載があります。
A. いいえ、評価者は暗号化されたデータにしかアクセスできないため、データ処理者としての資格を満たしていません。
B. いいえ。評価者はデータを自らの施設にコピーしないため、データ処理者としての資格を満たしません。
C. はい。評価者は共同データ管理者とみなされ、相互のデータ処理契約に署名する必要があります。
D. はい、評価者はデータ処理者であり、個人データの処理は別の契約またはその他の法的行為によって規制される必要があります。
Answer: D (メーッセージを残す)
GDPR によれば、データ処理者とは、データ管理者に代わって個人データを処理する個人または団体を指します1。データ管理者とは、個人データの処理目的と手段を決定する者です1。データ処理契約 (DPA) は、データ保護に関する両当事者の権利と義務を定めた契約文書です2。GDPR では、データ処理者と契約するデータ管理者は、GDPR の第 28.3 条に定められた内容に沿って書面による契約または法的行為を締結する必要があります3。DPA には、処理の主題、期間、性質、目的、個人データの種類とデータ主体のカテゴリー、管理者の義務と権利などを明記する必要があります3。
このシナリオでは、企業は顧客の個人データ処理の目的と手段を決定するため、データ管理者となります。サイバーセキュリティ評価者は、企業に代わって顧客の個人データを処理するため、データ処理者となります。評価者は、暗号化されている場合でも個人データにアクセスでき、企業のために特定の技術サービスを提供します。したがって、評価者はGDPRを遵守するために、企業とDPAを締結する必要があります。DPAは、処理の範囲、性質、目的、実施すべきセキュリティ対策、データ侵害発生時の通知手順、そして両当事者の権利と義務を規定します。参考文献 :1 :GDPR第4条2 :
データ処理契約 テンプレート）- GDPR.eu3: GDPR の第 28 条。

最新問題: **134**
シナリオ
次の質問に答えるには、以下を使用してください。
ARRAホテルズにとって、財務的には非常に好調な一年となりました。ギリシャ 5)、イタリア 15)、スペイン 1)にある21のホテルは、過去最高の収益を記録しました。この成果を祝うため、イタリア本社に拠点を置くARRAホテルズの人事部は、スペインのホテルで420名の従業員とその家族を対象としたチームイベントを開催しました。
ホテルに到着すると、従業員とそのご家族全員に受付で電子リストバンドが渡されます。このリストバンドにはいくつかの機能があります。
ホテルの「パーティーゾーン」へのアクセスを許可し、ユーザーが許可されていないエリアに近づくとブザーを鳴らします。
法定年齢の人1人につき最大3杯まで無料でドリンクをお楽しみいただけます。この制限に達すると、ブザーが鳴ります。
企画されているゲームやコンテストに参加するための固有のID番号を付与します。
リストバンドと一緒に、各ゲストにQRコードが配布されます。このQRコードをクリックすると、リストバンドの使用に関するオンラインプライバシー通知が表示されます。このページには、チェックが入っていない同意チェックボックスがあります。16歳未満の従業員の家族の場合は、親の同意が必要です。
イベントのために計画されたさまざまなアクティビティの中で、ARRA ホテルの人事部は、メインイベント会場とは別に、従業員が伝統的なカーニバルの衣装を着て写真を撮ることができるフォトコールエリアを自主的に設置しました。
写真は一般的なマーケティングの目的で ARRA Hotels のメイン Web サイトに掲載されます。
事件発生当夜、ARRA傘下のギリシャのホテル従業員が、自分が写った写真の出来栄えに不満を抱き、以下の点について監督当局に苦情を申し立てる意向を示しました。

別個のフォトコールエリアにプライバシーに関する通知がない
個人データの違法な国境を越えた処理
彼の写真の受け入れ難い美的結果
個人データを含むフォトコール写真の処理において、次の原則のうちどれが違反されている可能性がありますか?
A. 透明性。
B. 適切性。
C. 法の遵守。
D. データの最小化。
Answer: (解答を表示する)

最新問題: **135**
ある企業が、欧州連合/EEA 以外の国に個人データを転送したいと考えています。そのために、その国の法律と慣行の評価を計画していますが、これらが自社が使用しようとしている転送保護手段に影響を及ぼす可能性があることを承知しています。次のすべての要素は、企業が検討する必要がある要素のうち、どれを除くか?
A. 移転される個人データにアクセスする可能性のある第三国の当局が利用できる技術的、財政的、および人的資源
B. 欧州連合/EEAに設立されたデータ管理者または処理者と、関係する第三国に設立された移転の受取人との間の契約条項
C. 関係する第三国における近代化のプロセスと、個人データの国際移転に依存する新興技術へのアクセス
D. 同じ国または別の第三国のサブプロセッサーへの個人データの転送など、あらゆる転送。
Answer: C (メーッセージを残す)

最新問題: **136**
シナリオ
次の質問に答えるには、以下を使用してください。
ARRAホテルズにとって、財務的には非常に好調な一年となりました。ギリシャ (5)、イタリア (15)、スペイン (1)にある21のホテルは、過去最高の収益を記録しました。この成果を祝うため、イタリア本社に拠点を置くARRAホテルズの人事部は、スペインのホテルで420名の従業員とその家族を対象としたチームイベントを開催しました。
ホテルに到着すると、従業員とそのご家族全員に受付で電子リストバンドが渡されます。このリストバンドにはいくつかの機能があります。
ホテルの「パーティーゾーン」へのアクセスを許可し、ユーザーが許可されていないエリアに近づくとブザーを鳴らします。
法定年齢の人1人につき最大3杯まで無料でドリンクをお楽しみいただけます。この制限に達すると、ブザーが鳴ります。
企画されているゲームやコンテストに参加するための固有のID番号を付与します。
リストバンドと一緒に、各ゲストにQRコードが配布されます。このQRコードをクリックすると、リストバンドの使用に関するオンラインプライバシー通知が表示されます。このページには、チェックが入っていない同意チェックボックスがあります。16歳未満の従業員の家族の場合は、親の同意が必要です。
イベントのために計画されたさまざまなアクティビティの中で、ARRA ホテルの人事部は、メインイベント会場とは別に、従業員が伝統的なカーニバルの衣装を着て写真を撮ることができるフォトコールエリアを自主的に設置しました。
写真は一般的なマーケティングの目的で ARRA Hotels のメイン Web サイトに掲載されます。
事件発生当夜、ARRA傘下のギリシャのホテル従業員が、自分が写った写真の出来栄えに不満を抱き、以下の点について監督当局に苦情を申し立てる意向を示しました。

別個のフォトコールエリアにプライバシーに関する通知がない
個人データの違法な国境を越えた処理
彼の写真の受け入れ難い美的結果
なぜ同意はパーティーゾーンにアクセスするための十分な法的根拠とみなされないのでしょうか?
A. 同意が完全に明確ではありません。
B. 十分な情報に基づいた同意ではありません。
C. 同意は自由に与えられたものではありません。
D. 同意は書面ではありません。
Answer: C (メーッセージを残す**)**
GDPRに基づく個人データ処理の法的根拠の一つは同意ですが、有効となるには一定の条件を満たす必要があります。GDPR第4条11項によれば、同意とは データ主体が、自らの意思を表明し、自由に与えられた、具体的で、十分な情報に基づいた、かつ明確な意思表示であり、これによりデータ主体は、声明または明確な肯定的行為によって、自己に関する個人データの処理に同意する旨を表明する」ことを意味します。このシナリオでは、同意は自由に与えられたものではないため、パーティーゾーンへのアクセスの適切な法的根拠とはみなされません。自由に与えられた同意とは、データ主体が処理に同意するかしないかを真に自由に選択できること、そしてデータ主体が同意しない場合でも不利益、強制、または重大な悪影響がないことを意味します。しかし、この場合、同意はパーティーゾーンへのアクセスを条件としており、これがイベントの主目的です。したがって、データ主体は実質的な選択肢を持たず、イベントに参加するために同意しなければならないというプレッシャーや義務を感じる可能性があります。これは自由同意の原則に違反しており、法的根拠としての同意が無効になる可能性があります。
参照：
* GDPR第4条 - 定義1
* GDPR第7条 - 同意の条件2
* 規則2016/6793に基づく同意に関するガイドライン05/2020

最新問題: **137**
ある民間企業は、フランス、ポーランド、イギリス、そして本社所在地であるドイツに拠点を有しています。同社は世界中でサービスを提供しています。サービスの大部分はドイツで設計され、他の拠点でサポートされています。しかし、サービスの一つであるSaaS $oftware as a Service）アプリケーションは、ポーランドの拠点で定義 実装され、他の拠点でもサポートされています。
SaaS サービスの主たる監督機関は何ですか?
A. ドイツの連邦レベルの監督機関。
B. ドイツの地域レベルの監督機関。
C. ポーランド共和国の監督機関。
D. 欧州連合の監督機関。
Answer: C (メーッセージを残す**)**

GDPR では、処理活動に関連する主要な施設の所在地によって主たる監督機関が決定されます。
このケースでは、会社の本社はドイツにあるにもかかわらず、SaaSアプリケーションはポーランドの事業所によって具体的に定義・実装されました。これは、当該SaaSサービスに関連する個人データの処理目的と手段を決定する上で、ポーランドの事業所が主導的な役割を担っていることを示しています。
したがって、ポーランドの監督機関がこの特定の処理活動の主たる監督機関となります。
参考文献:
* GDPR第56条 - 主たる監督当局の権限
* IAPP CIPP/E教科書、第3章 :EU一般データ保護規則（特に、ワンストップショップメカニズムと主導監督機関に関するセクション）

最新問題**: 138**
多国籍企業が、ヨーロッパに拠点を置く従業員を含むすべての現従業員および潜在的な従業員に対して身元調査を実施したい場合、その企業はどのような重要な規定に従う必要がありますか?
A. 従業員の身元調査は、すべての従業員に事前に通知した場合にのみ実行できます。
B. 身元調査は、ヨーロッパに拠点を置く従業員を含むすべての従業員からの事前の通知と明示的な同意がある場合にのみ許可されます。
C. 欧州の従業員に対する身元調査は、データ保護法と雇用法に基づいて行われますが、加盟国によって異なる場合があります。
D. ヨーロッパの従業員に対する身元調査は許可されない可能性がありますが、企業は正当な利益に基づいてリストを作成し、雇用に不適格な個人を特定することができます。
Answer: C (メーッセージを残す**)**
参考 :https://www.shrm.org/resourcesandtools/tools-and-samples/toolkits/pages/conductingbackgroundinvestigations.aspx

最新問題**: 139**
GDPR によれば、詐欺防止の目的で個人データを処理したいオンライン ショップにとって最も適切な法的根拠はどれでしょうか?
A. 同意
B. 正当な利益
C. データ主体の利益の保護。
D. コンタクトのパフォーマンス
Answer: (解答を表示する**)**

最新問題**: 140**
EU のデータ保護法執行指令に基づき、政府は、法律で定められ、必要かつ適切な措置である限り、個人データに関する秘密の調査を行うことができます。
A. 慎重だ。
B. 比例する。
C. DPA 承認済み。
D. 重要です。
Answer: B (メーッセージを残す**)**

最新問題**: 141**
シナリオ

次の質問に答えるには、以下を使用してください。
Building Block Inc.はシカゴに本社を置き、米国、アジア、ヨーロッパ（ドイツ、イタリア、フランス、ポルトガルを含む）にオフィスを構える多国籍企業です。昨年、同社はフィッシング攻撃の被害に遭い、大規模なデータ漏洩が発生しました。取締役会は、ゼネラルマネージャー、プライバシーオフィス、情報セキュリティチームと連携し、追加のセキュリティ対策を講じることを決議しました。これには、トレーニングによる意識向上プログラム、サイバーセキュリティ監査、そしてSecurityScanと呼ばれる新しいソフトウェアツールの導入が含まれます。SecurityScanは、従業員のコンピュータをスキャンし、ベンダーによるサポートが終了してセキュリティアップデートが提供されていないソフトウェアがないか確認します。このソフトウェアは、従業員のコンピュータの監視など、他の機能も備えています。
これらの対策は従業員に影響を及ぼす可能性があるため、Building Block のプライバシー オフィスは、情報セキュリティを強化し、将来のデータ侵害を防止するための一連の取り組みを実施することを通知する一般通知を全従業員に発行することを決定しました。
これらの対策を実施した後、サーバーのパフォーマンスが低下しました。ゼネラルマネージャーはセキュリティチームに対し、SecurityScanを使用して従業員のコンピュータのアクティビティと位置情報を監視する方法を指示しました。この作業中、情報セキュリティチームは、イタリア出身の従業員が映画のビデオライブラリに毎日接続していること、またドイツ出身の従業員が許可なくリモートワークを行っていることを発見しました。セキュリティチームはこれらのインシデントをプライバシーオフィスとゼネラルマネージャーに報告しました。報告書では、イタリア出身の従業員がサーバーのパフォーマンス低下の原因であると結論付けられました。
これらの違反行為の重大性を考慮し、同社のセキュリティおよびプライバシーポリシーでは、従業員が会社のコンピュータにソフトウェアをインストールしたり、許可なくリモートワークしたりすることを禁止しているため、同社は両従業員に懲戒処分を適用することを決定しました。
監視の目的、データの潜在的な用途、プライバシー権について従業員に通知することに加えて、セキュリティ対策を実施する前に、Building Block は従業員にどのような情報を提供するべきでしたか?
A. 雇用契約書に規定されている内容に関する情報。
B. 従業員が質問がある場合に連絡すべき相手に関する情報。
C. 同意を与えることが従業員にどのような影響を与えるかについての情報。
D. 対策が会社にとってどのように最善の利益となるかについての情報。
Answer: (解答を表示する**)**
GDPR によれば、データ主体から個人データを収集する場合、管理者はデータ主体に対して、管理者の身元および連絡先、データ保護責任者の連絡先、処理の目的および法的根拠、個人データの受領者または受領者の区分、データ主体の権利、および公正かつ透明な処理を確保するために必要なその他の情報などの特定の情報を提供しなければなりません1。この情報は、明確で平易な言葉を使用して、簡潔で透明性があり、理解しやすく、簡単にアクセスできる形式で提供されなければなりません2。したがって、Building Block は、セキュリティ対策を実施する前に、情報通知の一部として、データ保護責任者やプライバシー オフィスなど、監視に関する質問がある場合に連絡できる連絡先についての情報を従業員に提供すべきでした。これにより、従業員は、個人データの処理へのアクセス、修正、消去、制限、または異議申し立ての権利、あるいは監督機関に苦情を申し立てる権利などの権利を行使できるようになります3。参照: 1 Art. 13 GDPR - データ主体から個人データを収集する場合に提供される情報 - 一般データ保護規則 (GDPR)2 条。12 GDPR - データ主体の権利を行使するための透明な情報、コミュニケーション、方法 - 一般データ保護規則 (GDPR)3 条。15-22 GDPR - データ主体の権利 - 一般データ保護規則 (GDPR)。

最新問題**: 142**

SCENARIO
Please use the following to answer the next question:
ProStorageは、オランダに本社を置く多国籍クラウドストレージプロバイダーです。CEOのルース ･ブラウン氏は、成長のために2本柱の戦略を立てました。1) ProStorageの顧客ベースを世界中に拡大し、2) 効果的なチームを効率的に採用してProStorageの営業部隊を増強することです。この戦略の実行は、ルースの健康状態により、最近、労働時間が制限され、潜在顧客に会うために出張することも困難になったため、複雑になっています。ProStorageの人事部とルースの首席スタッフは現在協力して、彼女のスケジュールを管理し、彼女がすべての医療予約を確実に受けられるようにしています。後者は、ルースが前回インドを旅行した際に健康上の緊急事態に見舞われ、ニューデリーで入院して以来、特に重要になっています。ルースの家族と連絡が取れなかったため、病院はProStorageに連絡し、首席スタッフと連絡を取ることができました。首席スタッフは、人事部長のメアリーと連携していました。
ルースが ProStorage を始めたときに出したリクエストに応じて、医師に情報を提供しました。より多くの営業担当者を雇うというルースの戦略目標をサポートするために、人事チームは、新しい従業員の募集、面接、雇用、オンボーディングを効率的に行うためのプロセスの改善に注力しています。これを支援するため、メアリーはドイツを拠点とする HRYourWay とオーストラリアを拠点とする InstaHR という 2 つのベンダーを特定しました。彼女は、ルースと協力して最終決定を下せるよう、両方のベンダーに ProStorage のベンダーリスクレビュープロセスを実行してもらうことにしました。レビュープロセスの一部として、ProStorage のプライバシープログラムの維持 (コントローラー BCR の維持とベンダーリスク評価の実施を含む) を担当しているジャッキーが両方のベンダーをレビューしましたが、移管影響評価は InstaHR についてのみ完了しました。彼女のレビュー後、どちらもより確立されたプライバシープログラムを誇り、サードパーティの認証を提供していましたが、HRYourWay はデータ保護操作が最小限の小規模ベンダーでした。
そこで彼女はInstaHRを勧めました。
ProStorageのマーケティングチームは、市場シェア拡大が必要な業界に注力することで、同社の戦略目標の達成にも取り組みました。この取り組みを支援するため、チームは金融業界の顧客と深い関係を持つ米国企業であるUpFinanceをパートナーとして選定しました。ProStorageのデューデリジェンスプロセスにおいて、プライバシーチームのジャッキーは、移転影響評価において、UpFinanceがエンドツーエンドの暗号化（暗号鍵は顧客が保有）を含む複数のデータ保護対策を実施していることを指摘しました。
注目すべきことに、UpFinanceは創業7年間、政府からの要請を一度も受けていません。それでもジャッキーは、UpFinanceが代理で処理する個人データについて政府から要請を受けた場合、当該データを開示する前にProStorageに通知することを契約に盛り込むことを推奨しました。
InstaHR を使用する場合、Jackie はどのような転送メカニズムを推奨しますか?
A. 適切性
B. 拘束力のある企業規則。
C. 従業員の明示的な同意。
D. 標準契約条項
Answer: D (メーッセージを残す)
GDPR によれば、第三国または国際組織への個人データの転送は、委員会による十分性の決定、データの輸出者と輸入者による適切な保護措置、または特定の状況に対する特例に基づく必要があります1。このシナリオでは、InstaHR はオーストラリアに拠点を置く会社で、オランダに拠点を置く会社 ProStorage に代わって個人データを処理します。オーストラリアは委員会によって十分なレベルのデータ保護を提供する国として認められていないため2、十分性のオプションは利用できません。拘束的企業準則 (BCR) は、多国籍企業または組織グループが採用する内部規則であり、同じ企業グループ内の個人データを十分なレベルの保護を提供していない国にある事業体に国際的に転送することに関するグローバル ポリシーを定義します3。ただし、InstaHR は ProStorage と同じ企

業グループの一部ではないため、この場合は BCR は適用されません。従業員の明示的な同意は、特定の状況においては例外となる可能性がありますが、自由意思によるものであり、具体的で、十分な情報に基づいた明確な同意でなければならず、いつでも撤回できるため、信頼性が高く実用的な移転メカニズムではありません4。したがって、InstaHRを使用するのに最適な移転メカニズムは、標準契約条項（SCC）です。SCCは、欧州委員会によって事前承認された契約条項であり、EU/EEAから第三国に個人データを移転する際に、データ保護のための適切な保護手段を提供します。SCCは法的拘束力を持ち、データ主体によって執行可能であり、データの輸出者と輸入者の両方に義務を課します。SCCは、GDPRに基づく移転メカニズムとして、データ管理者とデータ処理者によって広く使用されています。参考文献：1：GDPR第44条 - 移転に関する一般原則2：十分性認定 欧州委員会3：拘束的企業準則 欧州委員会4：GDPR第7条：標準契約条項（SCC） - 欧州委員会1.

最新問題: **143**
GDPR第13条および第14条は、個人データを収集する際にデータ管理者がデータ主体に通知する義務について詳細に規定しています。ただし、両条とも、データ主体が既に情報を保有している場合については例外を規定しています。
他にどのような状況でデータ管理者が第 14 条に基づくこの義務から免除されるでしょうか?
A. 個人データがパブリックドメインの複数のソースから取得された場合
B. 情報を提供することが警察の命令に反する場合。
C. 情報提供に過度の労力がかかる場合
D. GDPR発効の5年前に個人データが取得された場合
Answer: (解答を表示する)

最新問題: **144**
シナリオ
次の質問に答えるには、以下を使用してください。
TripBliss Inc.は、ここ数年で大幅な収益減少に陥っている旅行サービス会社です。新任マネージャーのオリバーは、その一因として会社のウェブサイトの老朽化が考えられます。調査を行った後、彼は新興IT企業Techivaの営業担当者と面談し、TripBliss Inc.の経営難に陥った事業のために、最先端のウェブサイトを新たにデザインしてくれることを期待します。
交渉中、Techiva の担当者は、詳細なアンケートを通じてより多くの顧客情報を収集する計画について説明します。この情報は、顧客の好みを特定の旅行先に合わせて調整するために使用できます。
TripBliss Inc.は、年齢、収入、民族など、目標達成に最も役立つデータカテゴリーをいくつでも選択できます。オリバーはこのアイデアに満足していますが、アンケートでは顧客からデータ収集への明示的な同意を得る必要があるため、このアプローチの成功度を測る方法も必要です。Techivaの担当者は、顧客がどのようにウェブサイトを利用しているかをより深く理解するために、新しいウェブサイトのトラフィックを分析するプログラムも実行することを提案しました。担当者は、顧客のデバイスに複数のCookieを配置する計画を説明します。これらのCookieにより、TripBliss Inc.はIPアドレスやその他の情報を収集できます。例えば、顧客がどのサイトからアクセスしたか、TripBliss Inc.のウェブサイトで過ごした時間、どのページを訪問したかなどです。これらの情報はすべてログファイルにまとめられ、Techivaが専用のプログラムで分析します。TripBliss Inc.は、ウェブサイトの効果を評価するために、集計統計情報を受け取ります。オリバーは、これらのサービスをTechivaに積極的に依頼しています。
Techiva社は、プロジェクトの分析部分を長年のアカウントマネージャーであるレオン・サントスに割り当てました。通常の業務手順通り、レオンにはTripBliss社のウェブサイトの管理者権限が与えられ、そこから収集されたログファイルへのアクセスを許可できます。しかし、TripBliss社にとって残念なことに、レオンがこの新しいプロジェクトを引き受けたのは、Techiva社への不満が最高潮に達していた時期でした。会社から不当な扱いを受けたと感じたレオンは、復讐のため、趣味でハッカーをしている友人のフレッドに

助けを求めました。二人は協力して、フレッドにTechiva社のシステムにハッキングし、ログファイルをUSBメモリにコピーさせるという計画を立てました。当初はTechiva社を非難するために、USBメモリを報道機関とデータ保護当局に送るつもりでしたが、レオンは良心の呵責に襲われ、計画を再考することにしました。彼はUSBメモリからすべてのデータを安全に消去し、会社のアクセス制御システムを見直す必要があると上司に伝えることにしました。
レオンがマネージャーに通知した後、プロセッサーとしての Techiva の法的責任は何ですか?
A. TripBliss Inc. に報告する必要があります。
B. 完全なシステム監査を実施する必要があります。
C. 監督当局に報告しなければなりません。
D. ウェブサイトを利用した顧客に通知する必要があります。
Answer: A (メーッセージを残す**)**
GDPR第33条によれば、処理者は個人データ漏洩を認識した後、遅滞なく管理者に通知しなければなりません1。レオンとフレッドはデータを他者に開示していませんでしたが、ログファイルへの不正アクセスとコピーは依然として個人データ漏洩を構成します2。したがって、処理者であるTechivaは、管理者であるTripBliss Inc.に報告する法的責任を負います。その他の選択肢は、グッドプラクティスや契約条件となる場合がありますが、処理者にとって法的義務ではありません。参考文献：
* 無料のCIPP/E学習ガイド、32ページ、セクション4.1.2
* CIPP/E認証、27ページ、セクション4.1.2
* Cipp-e 学習ガイド、授業ノートと要約、38 ページ、セクション 4.1.2
* 新しいIAPP CIPP-E試験練習問題、質問141
* 処理者の責任、第2項

最新問題**: 145**
GDPR では、個人データを収集する前に、データ主体にどのような重要な情報を提供しなければならないのでしょうか?
A. コントローラーがデータを収集する権限と、データが送信される第三者。
B. 関係する政府機関の名前とデータの修正に必要な手順。
C. 管理者の ID と連絡先の詳細、およびデータが収集される理由。
D. コントローラーの連絡先情報と保持ポリシーの説明。
Answer: (解答を表示する**)**
説明/参照: https://gdpr-info.eu/art-13-gdpr/

最新問題**: 146**
データ保護責任者を任命した後、データ管理者またはデータ処理者にはどのような義務がありますか?
A. データ保護責任者が定義されたタスクの遂行に関して十分な指示を確実に受けられるようにするため。
B. データ保護責任者の定義されたタスクを実行し、専門知識を維持するために必要なリソースを提供します。
C. データ保護担当者が個人の質問に対する唯一の連絡先として機能することを保証するため:
個人データについて。
D. 組織の慣行を管理し、データ保護の原則への準拠を証明するための行動規範をデータ保護責任者に提出し、承認を得る。
Answer: (解答を表示する**)**
英国GDPRによれば、管理者および処理者は、データ保護責任者が第39条に規定する業務を遂行できるよう、当該業務の遂行に必要なリソース、個人データおよび処理業務へのアクセス、ならびにデータ保護責任者の専門知識の維持に必要なリソースを提供するこ

とにより、データ保護責任者を支援しなければならない1。また、管理者および処理者は、データ保護責任者がこれらの業務の遂行に関していかなる指示も受けないこと、およびデータ保護責任者が管理者または処理者の最高経営責任者に直接報告することを確保しなければならない1。
参考: https://www.i-scoop.eu/gdpr/data-controller-data-controller-duties/

最新問題**: 147**
シナリオ
次の質問に答えるには、以下を使用してください。
ベッドロック保険の長年の顧客であるルイスさんは、数ヶ月前に軽微な交通事故に遭いました。けが人はいませんでしたが、ルイスさんは 「アクシデンタブル」という会社から、人身傷害の賠償金回収を支援するという内容のメッセージや電話に悩まされています。
保険会社が顧客のデータを第三者に販売していると聞いていたルイスさんは、「アクシデンタブル」がベッドロック保険から自分の情報を入手したに違いないと確信しています。
ルイはまた、ベッドロック社からあらゆる種類の保険を売りつけようとするマーケティング情報をますます多く受け取るようになった。
これに動揺したルイは、インターネットの価格比較サイトを調べ始めました。長年ベッドロックの忠実な顧客であったにもかかわらず、他の保険会社がベッドロックよりもはるかに安い保険料を提示していることに気づき、衝撃を受けました。ベッドロックの保険の更新時期が来たとき、彼はザントルム保険に乗り換えることにしました。
In order to activate his new insurance policy, Louis needs to supply Zantrum with information about his No Claims bonus, his vehicle and his driving history. After researching his rights under the GDPR, he writes to ask Bedrock to transfer his information directly to Zantrum. He also takes this opportunity to ask Bedrock to stop using his personal data for marketing purposes.
Bedrock supplies Louis with a PDF and XML (Extensible Markup Language) versions of his No Claims Certificate, but tells Louis it cannot transfer his data directly to Zantrum as this is not technically feasible. Bedrock also explains that Louis's contract included a provision whereby Louis agreed that his data could be used for marketing purposes; according to Bedrock, it is too late for Louis to change his mind about this. It angers Louis when he recalls the wording of the contract, which was filled with legal jargon and very confusing.
In the meantime, Louis is still receiving unwanted calls from Accidentable Insurance. He writes to Accidentable to ask for the name of the organization that supplied his details to them. He warns Accidentable that he plans to complain to the data protection authority, because he thinks their company has been using his data unlawfully. His letter states that he does not want his data being used by them in any way.
Accidentable's response letter confirms Louis's suspicions. Accidentable is Bedrock Insurance's wholly owned subsidiary, and they received information about Louis's accident from Bedrock shortly after Louis submitted his accident claim. Accidentable assures Louis that there has been no breach of the GDPR, as Louis's contract included, a provision in which he agreed to share his information with Bedrock's affiliates for business purposes.
Louis is disgusted by the way in which he has been treated by Bedrock, and writes to them insisting that all his information be erased from their computer system.
Which statement accurately summarizes Bedrock's obligation in regard to Louis's data portability request?
A. Bedrock has failed to comply with the duty to transfer Louis's data to Zantrum because it has an obligation to develop commonly used, machine-readable and interoperable formats so that all customer data can be ported to other insurers on request.
B. Bedrock does not have a duty to transfer Louis's data to Zantrum if doing so is legitimately not technically feasible.

C. Bedrock does not have to transfer Louis's data to Zantrum because the right to data portability does not apply where personal data are processed in order to carry out tasks in the public interest.
D. Bedrock has failed to comply with the duty to transfer Louis's data to Zantrum because the duty applies wherever personal data are processed by automated means and necessary for the performance of a contract with the customer.
Answer: C (メーッセージを残す)

最新問題**: 148**
シナリオ
次の質問に答えるには、以下を使用してください。
従業員数が急速に増加したため、A 社は給与計算業務を B 社にアウトソーシングすることを決定しました。
B 社は、大規模な顧客基盤を持ち、業界で確固たる評判を誇る、定評のある給与計算サービスプロバイダーです。
B社がA社向けに提供する給与計算ソリューションは、A社の各工場に設置された生体認証入退室システムから得られる勤怠データの収集に依存しています。B社は生体認証データを保有しませんが、関連データはB社の英国サーバーにアップロードされ、給与計算サービスの提供に使用されます。B社の本番システムには、A社の従業員一人ひとりに関する以下の情報が保存されます。
* 名前
* 住所
* 生年月日
* 給与番号
* 国民保険番号
* 病気休暇手当の受給権
* 出産手当/育児手当の受給資格
* 休暇の権利
* 年金および給付金拠出金
* 労働組合の寄付
ジェニーは A 社のコンプライアンス担当者です。彼女はまず、A 社が新しい勤怠システムに関連してデータ保護影響評価を実施する必要があるかどうかを検討しましたが、それが必須かどうかはわかりません。
しかし、ジェニーはGDPRに基づき、B社に対し、勤怠データを給与計算サービスの提供目的にのみ使用し、データ保護のために適切な技術的および組織的なセキュリティ対策を講じることを義務付ける正式な書面による契約が必要であることを知っています。ジェニーはB社に対し、自社のデータ保護責任者（DPO）から助言を受けることを提案します。B社にはDPOはいませんが、契約締結のため、条項の全てに同意することに同意します。A社は契約を締結します。
数週間後、B社はA社との契約期間中に、給与計算サービスの機能強化を目的とした別のプロジェクトに着手し、C社に協力を依頼しました。C社は、B社の新しいデータベースを作成するために、B社の稼働中のシステムからすべての個人データを抽出することに同意しました。
このデータベースは、C社の米国サーバー上にホストされたテスト環境に保存されます。データはITテストの目的にのみ使用されるため、両社はサービス契約にデータ処理に関する条項を含めないことに合意しています。
残念ながら、C社の米国サーバーは時代遅れのITセキュリティシステムでしか保護されておらず、C社がプロジェクトに着手して間もなくサイバーセキュリティインシデントに見舞われました。その結果、A社の従業員に関するデータがC社のウェブサイトにアクセスするすべての人に公開されてしまいました。A社は、その後の調査に関連してジェニーが監督当局から書簡を受け取るまで、この事実を知りませんでした。
ジェニーは侵害に気づくとすぐに、影響を受ける従業員全員に通知します。

GDPRでは、企業が適切な技術的および組織的対策を実施できる能力を十分に保証することが求められています。B社がこの要件を満たす最も現実的な方法は何でしょうか？
A. 認定機関の勧告に沿った対策を実施している企業を採用します。
B. A 社の IT チームにアドバイスと技術サポートを依頼します。
C. 自社のサービスを改善するために他社のデータを利用することを避ける。
D. 適切な監督当局とともに企業の対策を審査する。
Answer: A (メーッセージを残す)
* GDPR1234の第82条は、GDPRの違反の結果として物質的または非物質的損害を被った人物に対する賠償および責任の権利を規定しています。
* 第 821234 条の第 4 項では、管理者または処理者は、損害の原因となった事象についていかなる責任も負わないことを証明した場合、第 2 項 (GDPR に違反する処理によって生じた損害に対する責任を負わせる) に基づく責任を免除されると規定されています。
* したがって、GDPR に基づく賠償および責任の権利では、データ管理者 (またはデータ処理者) が損害の原因となった事象に対して一切の責任を負わないことを証明した場合、責任が免除されます。
参考文献:
1: GDPR第82条 - 補償および責任の権利 - 一般データ保護規則（GDPR）
2 :GDPR第82条 - 補償および責任の権利 - GDPR.eu
3: GDPR第82条: 補償および責任の権利 - Advisera
4: GDPR第82条 | 補償および責任の権利
参考 :https://www.knowyourcompliance.com/gdpr-technical-organisational-measures/

最新問題**: 149**
一般データ保護規則の適用範囲外となるデータの種類は何ですか?
A. 仮名
B. 匿名
C. 暗号化
D. マスク
Answer: B (メーッセージを残す)
一般データ保護規則（GDPR）は、欧州連合（EU）および欧州経済地域（EEA）における個人の個人データの処理に適用されるデータ保護法です。個人データとは、氏名、住所、メールアドレス、電話番号など、特定された、または特定可能な自然人に関するあらゆる情報を指します12。GDPRは、匿名化された個人データ、つまり特定の個人に紐付けられない個人データには適用されません12。匿名化は、仮名の使用、データの集約または一般化、統計的手法の適用など、データから識別情報を削除またはマスキングすることで実現できます12。
したがって、GDPR の範囲外となるデータの種類は匿名化されたデータです。
参考資料: 1: 無料の CIPP/E 学習ガイド - 国際プライバシー専門家協会 2: CIPP/E 認定 - 国際プライバシー専門家協会

最新問題**: 150**
シナリオ
次の質問に答えるには、以下を使用してください。
環境に優しい靴で知られるオンライン小売業者Liemは、最近ヨーロッパでの事業を拡大しました。市場支配力の確立を目指し、Liemはベルトやバッグなどのアクセサリーを販売する同じく環境に優しい企業、EcoMickと提携しました。両社は協力し、製品の環境的

および経済的メリットを強調する一連のマーケティングキャンペーンを企画しました。数ヶ月にわたる計画の後、LiemとEcoMickは、それぞれの担当者にキャンペーンを送信するために、同じマーケティングデータベースMarketIQを使用するデータ共有契約を締結しました。
Liem 氏と EcoMick 氏は MarketIQ とデータ処理契約も締結しました。その契約条件には、Liem 氏と EcoMick 氏の指示に従ってのみ個人データを処理し、GDPR 義務の遵守を証明するために必要なすべての情報を Liem 氏と EcoMick 氏に提供することが含まれていました。
その後、リーム氏とエコミック氏は、機械学習を用いて企業のキャンペーン成功を支援するマーケティング最適化企業、JaphSoft社のサービスを導入しました。顧客は、各キャンペーンでターゲットにしたい個人の個人データをJaphSoft社に提供します。顧客データの保護を確実にするため、JaphSoft社は適切と判断した技術的および組織的措置を講じています。JaphSoft社は、顧客から受け取ったデータを分析することで、キャンペーン成功の鍵となる要素を特定し、機械学習モデルの継続的な改善に取り組んでいます。そして、そのモデルを用いて顧客ベースにサービスを提供しています。モデルは一定期間内により多くの情報を収集することでのみ改善されるため、JaphSoft社は顧客から受け取ったデータを削除するプロセスを設けていません。ただし、データプライバシー規則への準拠を確保するため、JaphSoft社は連絡先情報から個人識別情報を削除することで個人データを仮名化しています。ただし、JaphSoft社のエンジニアは、すべての連絡先情報を個人識別情報と同じデータベースに保管しています。
リーム社およびエコミック社との契約に基づき、JaphSoft社はMarketIQへのアクセスを取得しました。MarketIQには、連絡先情報と過去の購入履歴が含まれており、両社のウェブサイトの閲覧数を最大化するキャンペーンを作成するために利用されていました。
リーム社の以前の顧客であるイマン氏は、リーム社とエコミック社の最新製品に関するマーケティングキャンペーンをJaphSoft社から受け取りました。イマン氏は、リーム社の製品に関する情報を今後受け取るためのチェックボックスにチェックを入れたことは覚えていますが、エコミック社で買い物をしたことはなく、同社に個人情報を提供したこともありません。
Iman 氏による同意が JaphSoft に関して有効であるとみなされないのはなぜですか?
A. 彼女は、どの管理者が彼女の個人データを処理するのか知らされていませんでした。
B. 彼女は、Liem が提供したプライバシー通知の視覚的な表現のみを閲覧しました。
C. 彼女は、自分の個人データが共有されることを記載したプライバシー通知を読んでいませんでした。
D. 彼女は JaphSoft から購入したことはなく、同社との関係もありません。
Answer: (解答を表示する**)**
イマン氏による同意がJaphSoftに関して有効とみなされない理由は、彼女がEcoMickとの個人データの共有に同意しなかったからではなく、どの管理者が彼女の個人データを処理するのか知らされていなかったからです。JaphSoftは、個人データ処理の目的と手段を決定する管理者であり、マーケティング最適化モデルの改善と顧客へのより良いサービス提供を目的としています。JaphSoftは、個人データの本来の管理者であるLiem氏とEcoMick氏の指示のみに基づいて行動するのではなく、自社の利益と利益のためにデータを使用します。したがって、JaphSoftはイマン氏から別途同意を得るか、正当な利益などの別の法的根拠に基づいて彼女の個人データを処理すべきでした。イマン氏はJaphSoftではなくLiem氏に同意を与えただけで、彼女の個人データが別の管理者と共有または処理されることは知らされていませんでした。

最新問題**: 151**
OECDガイドライン、条約108、データ保護指令（指令95/46/EC）のすべてに共通しながらも、ヨーロッパではほとんど達成できなかった主要な目標は何ですか？
A. 正当なデータ処理基準のリストの確立
B. 法的拘束力のあるデータ保護原則の策定
C. データ保護へのアプローチの同期

D. 国境を越えたデータフローの制限
Answer: C (メーッセージを残す**)**
参考 https://ico.org.uk/media/about-the-ico/documents/1042349/review-of-eu-dp-directive.pdf (99)

最新問題**: 152**
シナリオ：
WeScanYouは、病院向けに診断ツールを提供する企業です。同社の製品「Scan4You」は、患者の画像データを分析して診断を導き出します。この製品は、欧州連合（EU）、英国、インド、オーストラリアのクリニックに販売されています。病院スタッフは、アイルランドにある中央サーバー上のウェブインターフェースを介してデータにアクセスします。
* 全世界の会社の中央管理はドイツにあります。
* オーストラリアの IT Development はシステムの設計と保守を行います。
* インドオフィスは、ガバナンス（保存期間など）を含む全体的なデータ戦略を設定します。
* フランスオフィスは、EU での実装と GDPR コンプライアンスの確保を担当します。
オーストラリアで発生した自然災害により、病院は患者のケアを優先せざるを得なくなりました。これを受けて、WeScanYouは、緊急度予測に基づいて患者の優先順位を自動的に決定し、それに応じて患者ファイルを並べ替える新しいAI機能を導入しました（ただし、その他の手動並べ替えオプションはそのままです）。
あるソフトウェアエンジニアは、この機能に反対（非倫理的だと考えている）し、システムを妨害して画像や自動診断結果を公開した。氏名や連絡先は記載されていなかった。
質問：
GDPR によれば、WeScanYou が新しい AI 機能を実装する際の主な問題は何ですか?
A. 自動化された意思決定に関する透明性の欠如。
B. 監督当局への事前協議を省略する。
C. 自動意思決定に対する同意を求めません。
D. 人間による介入の権利がない。
Answer: A (メーッセージを残す**)**
GDPR は、第 22 条 GDPR に基づいて自動意思決定を規制し、プロファイリングを含む自動処理のみに基づく、法的効果を生じさせたり個人に重大な影響を与えたりする意思決定から個人を保護します。
主な要件は次のとおりです。
* 透明性（GDPR 第 13 条～第 15 条）：管理者は、データ主体に対して、自動化された意思決定の存在、関連するロジック、およびその重要性と結果について通知する必要があります。
* 保護措置（GDPR第22条（3））：データ主体は、人間による介入を受け、自らの見解を表明し、決定に異議を申し立てることができる必要があります。

* 同意（第22条(2)(c)）：同意、自動化された意思決定が許可される法的根拠の1つですが、すべての場合に必須というわけではありません（例GDPR第9条(2)(h)に基づく医療目的のために必要な場合）。
* 事前協議（GDPR第36条）データ保護影響評価（DPIA）により軽減できない高いリスクが示された場合にのみ必要です。
この場合：
* AI機能は拘束力のある決定を下すものではありません（緊急度に基づいてファイルを分類しますが、代替の分類方法も残しています）。したがって、第22条に規定されている法的効果または類似の効果を持つ自動決定の禁止は直接適用されません。
* GDPR の主な問題は、WeScanYou が自動仕分けの仕組み、その目的、患者とスタッフへの潜在的な影響について透明性を確保する必要があることです。
* 事前協議 (B) は、DPIA で軽減不可能な高リスクが特定された場合にのみ関連しますが、ここでは主な懸念事項ではありません。
* 処理は他の法的根拠（例：医療の提供、公衆衛生に対する公共の利益）に依存する可能性があるため、同意（C）は厳密には必要ではありません。
* 手動による分類が依然として可能であるため、人間の介入 (D) がないわけではありません。
したがって、GDPRの主な問題は次のとおりです。
#自動化された意思決定に関する透明性の欠如 (オプション A)。
＃参照：
* GDPR 第22条、前文71-72（自動化された意思決定とプロファイリング）。
* GDPR 第 13 条～第 15 条（情報および透明性の義務）。
* CIPP/E 教科書 (第 3 版)、第 9 章「データ主体の権利」(情報および透明性の権利)、および第 7 章「合法的な処理基準」。

最新問題: **153**
シナリオ
次の質問に答えるには、以下を使用してください。
フィットネス企業Vigotronは最近、「M-Health」という新しいアプリを開発し、自社ウェブサイトから無料でダウンロードできるようにしたいと考えています。Vigotronのマーケティングマネージャーは、アシスタントのエミリーにアプリの説明と利用規約を明記したウェブページの作成を依頼しました。Vigotronに入社したばかりのエミリーは、この仕事に意欲的です。
前職でデータ保護に関する講座を受講したエミリーは、詳細は多少曖昧ではあるものの、Vigotronがアプリの利用に際してユーザーの同意を得る必要があるケースがあることを認識している。エミリーは、Vigotronの法務部門に提出する前に、可能な限り網羅した以下の草稿を作成した。
登録フォーム
Vigotron の新しい M-Health アプリを使用すると、食事、運動、睡眠パターンなど、さまざまな健康関連の活動を簡単に監視できます。M-Health は、スマートフォンの設定 (および既にインストールされている可能性のある他のサードパーティ製アプリ) に基づいて、これらすべての重要なライフスタイル要素に関するデータを収集し、生活の質を向上させるために必要な情報を提供します。(M-Health が提供するサービスの詳しい説明を読むには、ここをクリックしてください。) Vigotron はお客様のプライバシーを重視しています。M-Heaith アプリでは、アプリにどの情報を保存するか、どのアプリがデータにアクセスできるかを決めることができます。デバイスがパスコードでロックされている場合、すべての健康とフィットネスのデータはパスコードで暗号化されます。Health アプリに保存されたデータは、Vigotron のクラウド プロバイダーである Stratculous にバックアップできます。(Stratculous の詳細については、こちらをご覧ください。) Vigotron は、M-Health アプリで収集した個人情報を取引、貸与、または販売することはありません。さらに、当社は、裁判所の命令、召喚状の指示、またはメーカーの法的権利の執行や事業もしくは財産の保護の場合を除き、お客様の同意なしに、お客様の名前、メールアドレス、またはアプリから収集したその他の情報を第三者に提供することはありません。

M-Healthアプリは無料でご利用いただけます。ダウンロードしてご利用いただくには、まずこちらの登録フォームにご記入ください。 なお、M-Healthアプリのご利用は16歳以上の成人に限られます。ただし、未成年の方がご利用になる場合は、保護者の同意を得てください。）
* ファーストネーム：
* 姓:
* 生年：
* メールアドレス:
* 住所 オプション*)：
* 健康状態:
*お客様が関心をお持ちと思われる当社の製品およびサービスに関するニュースレターの受信をご希望の場合は、ご住所をご記入ください。後日、ニュースレターの受信を希望されない場合は、unsubscribe@vigotron.com までメールを送信いただくか、このページ下部に記載されている住所まで書面にて配信停止の旨をお送りください。
利用規約
1.管轄権。[...]
2.準拠法。[...]
3.責任の制限。[...]
同意
この登録フォームにご記入いただくことで、お客様は16歳以上であること、およびM-Healthアプリの利用を目的としてVigotronがお客様の個人データを処理することに同意するものとします。お客様は広告やマーケティングの配信を拒否する権利を有しますが、Vigotronがお客様に連絡を取ったり、サービスに関する必要な通知、契約、その他の情報をEメールまたはその他の電子的手段で提供したりすることに同意するものとします。また、お客様の健康に影響を与える可能性のあるM-Healthアプリの問題に関するアラートを、当社が自動送信することに同意するものとします。
エミリーはサムに草稿を送付し、レビューを依頼します。サムがエミリーの同意条項の最大の問題点として指摘する可能性が高いのは次のうちどれでしょうか？
A. 同意なしの健康状態に関する情報を要求するフィールドを含めることは違法です。
B. 健康データの処理には明示的な同意が必要ですが、フォームでは明示的な同意を求めていません。
C. ダイレクトマーケティングには明示的な同意が必要ですが、登録フォームでは異議申し立ての権利のみが規定されています。
D. フィットネス アプリの提供は、ダイレクト マーケティングのためのデータ処理への同意を条件とする必要があります。
Answer: C (メーッセージを残す)
GDPRによれば、個人データは特定され、明確かつ正当な目的のために収集されなければならず、それらの目的に反する方法でさらに処理されてはならないとされています1。つまり、データ管理者はデータ主体にデータ処理の目的を通知し、新たな目的または異なる目的については、データ主体の同意またはその他の法的根拠を得る必要があるということです2。
このシナリオでは、Brady社は顧客の個人データを、依頼されたサービスを履行するために、第三者委託業者であるHermes Designs社に転送しました。しかし、Hermes Designs社は顧客に開示されていない新たな目的、すなわちカスタマイズされたバナー広告のサンプル作成とダイレクトマーケティングの実施にデータを使用しました。これは目的限定の原則に違反しており、Brady社は法的リスクや顧客からの苦情に直面する可能性があります。
したがって、Brady は Hermes Designs による顧客の個人データの取り扱いに注意し、GDPR への準拠を確保するために適切な措置を講じる必要があります。
これがお役に立てば幸いです。他にご質問がございましたら、お気軽にお問い合わせください。#

1: GDPR第5条(1)(b) 2: GDPR第6条(4)

最新問題**: 154**
シナリオ
次の質問に答えるには、以下を使用してください。
Dynaroux Fashion（以下Dynaroux」）は、アイルランドのダブリンに本社を置き、約650名の従業員を擁する、国際的なオンライン衣料品小売業者です。ロナンは最近、同社のデータ保護責任者に任命され、一般データ保護規則（GDPR）およびその他のプライバシー法の遵守を監督しています。
同社は、子供を含むあらゆる年齢層を対象に、男性用と女性用の衣料品ラインを提供しています。その過程で、顧客の嗜好やクレジットカード番号や銀行口座番号といった機密性の高い金融情報など、大量の顧客情報を処理しています。
収益成長を積極的に図るため、CEOのジョナスはロナンに対し、顧客の購入履歴を分析することで顧客のプロファイリングに重点を置いた新しいモバイルアプリとロイヤルティプログラムを導入することを伝えた。ロナンはCEOに対し、(a) こうした活動には潜在的なリスクがあるため、ダイナルーはデータ保護影響評価を実施し、この新しい取り組みとプライバシーへの影響を評価する必要があること、(b) この評価結果が、適切な保護措置を講じない場合に高いリスクをもたらすことを示している場合、ダイナルーはアプリとロイヤルティプログラムを導入する前に、アイルランドのデータ保護コミッショナーと事前協議を行う必要がある可能性があることを伝えた。
ジョナス氏はロナン氏に対し、監督当局と直接交渉し、ディナルー社の事業計画や関連する処理活動の詳細を開示しなければならない可能性について不満を述べている。
Dynaroux に関する次の事実のうち、GDPR に基づくデータ保護影響評価のきっかけとなるものはどれですか?
A. 当社は、財務データや児童データなどの機密データカテゴリに関連する処理活動を実施します。
B. 当社は約 650 人の従業員を雇用しており、広範な処理活動を行う予定です。
C. 同社は顧客の購買パターンを分析し、顧客のプロファイリングを行う予定です。
D. 同社は、ビジネスモデルを転換し、オンラインショッピングに重点を置く予定です。
Answer: C (メーッセージを残す**)**
無料CIPP/E学習ガイドの14ページによると、「GDPRは、特に新しい技術を用いた処理、ならびに処理の性質、範囲、状況および目的を考慮した上で、自然人の権利および自由に高いリスクをもたらす可能性のある処理の種類について、管理者に対し、処理前にデータ保護影響評価（DPIA）を実施することを義務付けています。」GDPRはまた、DPIAが必要となる処理業務の例として、「プロファイリングを含む自動化された処理に基づき、自然人に関する個人的側面の体系的かつ広範な評価を行い、その評価に基づいて、自然人に関する法的効果を生じさせる、または同様に自然人に重大な影響を与える決定を行うもの」（第35条(3)(a)）を挙げています。したがって、Dynarouxが顧客の購買パターン分析を通じて顧客のプロファイリングを行う計画は、顧客に重大な影響を与える可能性のある自動化された処理に基づく個人的側面の体系的かつ広範な評価を伴うため、GDPRに基づくDPIAの対象となると考えられます。その他の選択肢は、有効な法的根拠の取得、適切な保護措置の提供、データ主体への通知など、GDPRに基づくその他の義務を伴う場合がありますが、必ずしもDPIAが必要となるケースではありません。参考：
無料のCIPP/E学習ガイド、14ページ
GDPR第35条

最新問題**: 155**
Please use the following to answer the next question:

Due to rapidly expanding workforce, Company A has decided to outsource its payroll function to Company B. Company B is an established payroll service provider with a sizable client base and a solid reputation in the industry.
Company B's payroll solution for Company A relies on the collection of time and attendance data obtained via a biometric entry system installed in each of Company A's factories. Company B won't hold any biometric data itself, but the related data will be uploaded to Company B's UK servers and used to provide the payroll service. Company B's live systems will contain the following information for each of Company A's employees:
Name
Address
Date of Birth
Payroll number
National Insurance number
Sick pay entitlement
Maternity/paternity pay entitlement
Holiday entitlement
Pension and benefits contributions
Trade union contributions
ジェニーは A 社のコンプライアンス担当者です。彼女はまず、A 社が新しい勤怠システムに関連してデータ保護影響評価を実施する必要があるかどうかを検討しましたが、それが必須かどうかはわかりません。
しかし、ジェニーはGDPRに基づき、B社に対し、勤怠データを給与計算サービスの提供目的にのみ使用し、データ保護のために適切な技術的および組織的なセキュリティ対策を講じることを義務付ける正式な書面による契約が必要であることを知っています。ジェニーはB社に対し、自社のデータ保護責任者（DPO）から助言を受けることを提案します。B社にはDPOはいませんが、契約締結のため、条項の全てに同意することに同意します。A社は契約を締結します。
数週間後、B社はA社との契約期間中に、給与計算サービスの機能強化を目的とした別のプロジェクトに着手し、C社に協力を依頼しました。C社は、B社の新しいデータベースを作成するために、B社の稼働中のシステムからすべての個人データを抽出することに同意しました。
このデータベースは、C社の米国サーバー上にホストされたテスト環境に保存されます。データはITテストの目的にのみ使用されるため、両社はサービス契約にデータ処理に関する条項を含めないことに合意しています。
残念ながら、C社の米国サーバーは時代遅れのITセキュリティシステムでしか保護されておらず、C社がプロジェクトに着手して間もなくサイバーセキュリティインシデントに見舞われました。その結果、A社の従業員に関するデータがC社のウェブサイトにアクセスするすべての人に公開されてしまいました。A社は、その後の調査に関連してジェニーが監督当局から書簡を受け取るまで、この事実を知りませんでした。ジェニーは侵害に気づき次第、影響を受ける全従業員に通知しました。
GDPRでは、企業が適切な技術的および組織的対策を実施できる能力を十分に保証することが求められています。B社がこの要件を満たす最も現実的な方法は何でしょうか？
A. 適切な監督当局とともに企業の対策を審査する。
B. 自社のサービスを改善するために他社のデータを利用することを避ける。
C. A 社の IT チームにアドバイスと技術サポートを依頼します。
D. 認定機関の勧告に沿った対策を実施している企業を採用します。
Answer: D (メーッセージを残す)

最新問題: **156**

シナリオ
次の質問に答えるには、以下を使用してください。
ABCホテルチェーンとXYZ旅行代理店は、米国を拠点とする多国籍企業です。両社は、マーケティング活動を統合するために、インターネットベースの共通プラットフォームを使用して顧客データを収集 -共有しています。さらに、両社は、保存するデータ、予約の受付方法と確認方法、そして保存データへのアクセス権について合意しています。
EU在住のマイクは、過去にXYZ旅行代理店を通じてABCホテルチェーンの宿泊施設に宿泊する旅行プランを予約したことがあります。XYZ旅行代理店は、会員登録するとポイントが貯まり、後日無料旅行と交換できるリワードプログラムを提供しています。マイクはリワードプログラム会員契約に署名しました。
マイクは、会社が自分の個人情報をどのように保有しているかを知りたいと考え、データ主体としての権利を行使するため、データへのアクセスを要求するメールを送信しました。
ABC ホテルチェーンと XYZ 旅行代理店が Mike のデータ アクセス要求に応じる必要がないのは、次のどの状況ですか。
A. 要求は、彼のプロフィール内の不正確な個人データにアクセスし、修正することです。
B. このリクエストは、リワード メンバーシップを処理するために個人データを受け取った受信者のアクセス権とカテゴリを取得することです。
C. 要求は、個人データの処理目的へのアクセスと情報の取得です。
D. リワード メンバーシップを維持しながら、個人データへのアクセスと消去を取得することを要求します。
Answer: (解答を表示する**)**

最新問題**: 157**
Planet 49 事件において、クッキーの問題に関して欧州連合司法裁判所 (CJEU) が下した主な判決は何でしたか?
A. ウェブサイトの Cookie に関する通知で、収集される情報と Cookie の有効期間が明確に示されている場合は、事前にチェックされたボックスが許容されます。
B. クッキーが個人データを追跡しない場合は、事前にチェックされたボックスが許容されます。
C. ePrivacy 指令で Cookie への同意が必要な場合は、GDPR の同意要件が適用されます。
D. データ主体が Cookie バナーを読んだ後も Web サイトをスクロールし続ける場合、このアクティビティは Cookie バナーに記載されている追跡に対する有効な同意を構成します。
Answer: (解答を表示する**)**

最新問題**: 158**
AI法によれば、高リスクAIシステムのプロバイダーには、以下の義務のうちどれか一つを除き、すべて義務があります。
A. システムがバイアスを軽減する方法をユーザーが理解していることを確認します。
B. システムを欧州 AI 委員会のデータベースに登録します。
C. システムに関する詳細なドキュメントをユーザーに提供します。
D. システムを市場に出す前に適合性評価を実施します。
Answer: A (メーッセージを残す**)**
EU人工知能法（AI法）は、安全性、公平性、透明性を確保するため、高リスクAIシステムに対する厳格な規制を導入しています。これらの規制は、EU内、さらには一定の条件下では世界的に、AIシステムの提供者と利用者の両方に適用されます。
AI法に基づく高リスクAIシステムのプロバイダーの主な義務には以下が含まれます。
* 適合性評価（回答選択肢D）

* 高リスクの AI システムを市場に投入する前に、プロバイダーは適合性評価を実施し、EU の法的および倫理的基準に準拠していることを確認する必要があります。
* 高リスクAIシステムの公開登録（回答選択肢B）
* AI法では、透明性と監視を強化するために、高リスクのAIシステムを欧州委員会が管理するEU全体のデータベースに登録することを義務付けています。
* 文書の提供（回答選択肢C）
* プロバイダーは、AI システムに関する詳細な技術文書をユーザーに提供し、システムの機能、リスク、コンプライアンス対策をユーザーが理解できるようにする必要があります。
回答選択肢Aが間違っているのはなぜですか?
AI法は、システムがどのようにバイアスを軽減するかを利用者に理解させることを、提供者に対して明示的に義務付けていません。代わりに、提供者は学習データとテストデータの品質を確保し、バイアスを防止するための安全策を講じる必要がありますが、これはバイアス軽減に関する利用者教育には適用されません。

最新問題: **159**
シナリオ
次の質問に答えるには、以下を使用してください。
ジョーは、DNA鑑定サービスを提供するカナダ企業Who-RUの新しいプライバシーマネージャーです。本社はモントリオールにあり、従業員全員がそこに勤務しています。同社はカナダ人のみにサービスを提供しています。ウェブサイトは英語とフランス語で提供され、カナダの通貨のみを受け付け、カナダ国外からのインターネットトラフィックをブロックしています ただし、この対策でカナダ国外からのトラフィックをすべてブロックできるわけではありません）。また、DNAレポートをカナダ国外に送付するよう要求する注文は処理せず、カナダ国外の返送先住所が記載されている注文は返品されます。
Who-RU の社長ボブ氏は、EU でこの製品に対する関心が非常に高いと考えており、同社は顧客基盤を拡大するためのさまざまな計画を検討しています。
最初の計画は、共同でWe-Track-Uと名付けられ、アプリを用いて既存のカナダの顧客基盤に関する情報を収集します。この拡張により、カナダの顧客は海外旅行中にアプリを使用できるようになります。ボブは、このアプリを用いて位置情報の収集を行うことを提案します。この計画が有望であれば、ボブはプッシュ通知とテキストメッセージを用いて既存顧客にEU版サービスの事前登録を促すことを提案します。ボブはこの作業計画をWe-Text-Uと呼んでいます。十分な事前登録数を集めた後、EU向けのコンテンツとサービスを開発する予定です。
もう1つのプランは「Customer for Life」と呼ばれる。これは、同社のアプリを通じて、DNA情報の保存や、他のアプリや医療機関との共有といった追加サービスを提供するという構想だ。同社の契約書には、顧客のDNAを無期限に保管し、新サービスの提供や顧客へのマーケティングに活用できることが明記されている。また、顧客はダイレクトマーケティングへの同意を撤回しないことに同意する、と明記されている。マーケティングディレクターのポール氏は、同社がこれらの条項を最大限に活用し、契約によって同意が無効となるため、顧客が同意を撤回しようとしても回避できると提案している。
最終計画は、EUにおけるブランドプレゼンスの構築です。同社はすでにこのプロセスに着手しており、ドイツにあるビルの命名権を購入する手続きを進めています。このビルには、Who-RUの幹部が海外旅行中に利用できるオフィススペースがいくつか設けられる予定です。このオフィスにはテクノロジーやインフラ設備は一切なく、机と椅子がいくつか置かれただけのシンプルな部屋です。
命名権契約に関する最近の出張中、ボブのノートパソコンが盗まれました。ノートパソコンには、Who-RUの顧客5,000人（全員カナダ在住）の暗号化されていないDNAレポートが保存されていました。レポートには、顧客名、生年月日、民族、人種的背景、親族名、性別、そして時折健康情報も含まれていました。

RU がラップトップの盗難について地元のドイツ DPA に通知する必要がないのはなぜですか?
A. 当社は、EU 内に設立された管理者ではありません。
B. このラップトップはカナダにある会社のものでした。
C. データは個人を特定できる財務情報とはみなされません。
D. 泥棒がラップトップ上のデータにアクセスしたという証拠はありません。
Answer: A (メーッセージを残す)
GDPRによれば、データ侵害は、当該侵害が自然人の権利と自由に対するリスクをもたらす可能性が低い場合を除き、管理者または処理者が所在する加盟国の監督機関に通知されなければなりません1。GDPRでは、管理者を 個人データの処理の目的と手段を単独で、または他者と共同で決定する自然人、法人、公的機関、代理店、その他の団体」と定義しています2。また、GDPRでは、管理者または処理者がEU域内で 安定した取引関係を通じて効果的かつ現実的に活動を行っている」場合、その法的形態や本社所在地に関わらず、EU域内に所在するものとみなされると規定されています3。
このシナリオでは、Who-RUはEU域内に設立された管理者ではありません。なぜなら、同社はEU域内に個人データ処理に関する安定した取引関係を有していないからです。同社はカナダ国民のみにサービスを提供しており、EU域内の個人をターゲットにしたり監視したりしていません。ドイツにあるビルの命名権を購入し、複数のオフィスを併設しているという事実は、EU域内における効果的かつ実質的な活動とはみなされません。なぜなら、これらのオフィスには個人データ処理のための技術やインフラが整備されておらず、幹部社員が海外旅行の際にのみ利用しているからです。したがって、Who-RUはGDPRのデータ侵害通知義務の対象ではなく、ノートパソコンの盗難についてドイツの現地DPAに通知する必要もありません。
参考文献:
GDPR第33条 - 監督機関への個人データ漏洩の通知 GDPR第4条 - 定義 GDPR第3条 - 適用範囲 GDPRに基づく個人データ漏洩通知に関するガイドライン9/2022 GDPRの適用範囲に関するガイドライン3/2018 GDPRとデータ漏洩通知についてご理解を深めていただければ幸いです。他にご質問がございましたら、お気軽にお問い合わせください。#

最新問題**: 160**
欧州データ保護委員会によると、EU データ保護法に基づく個人データの処理に関する原則に従わない概念または慣行は次のどれですか?
A. データ所有権の割り当て。
B. アクセス制御管理。
C. 頻繁な仮名化キーのローテーション。
D. 処理チェーンに沿ったエラーの伝播を回避します。
Answer: A (メーッセージを残す)
欧州データ保護委員会（EDI）によると、EUデータ保護法に基づく個人データ処理に関する原則は、合法性、公平性、透明性、目的の限定、データの最小化、正確性、保存期間の制限、完全性および機密性、そして説明責任です1。これらの原則は、アクセス制御管理、頻繁な仮名化キーのローテーション、処理チェーンにおけるエラー伝播の回避など、データ管理者とデータ処理者が遵守すべき特定の概念または慣行を暗示しています2。しかし、GDPRはデータ主体またはデータ管理者のいずれかによるデータ所有権の概念を認めていないため、データ所有権の割り当てはこれらの原則から導き出される概念または慣行ではありません3。
したがって、選択肢Aが正解です。参考文献：
* データ保護の基礎
* データ主体へのオンラインサービスの提供におけるGDPR第6条(1)(b)に基づく個人データの処理に関するガイドライン2/2019
* CIPP/E 学習ガイド、11 ページ

最新問題: **161**
主導監督機関 (LSA) の主な懸念事項はプライバシーのどの領域ですか?
A. 特別なデータカテゴリ
B. データアクセス紛争
C. データ主体の権利
D. 国境を越えた処理
Answer: (解答を表示する**)**

最新問題: **162**
スペインに拠点を置き、世界中でドキュメンタリーを撮影する著名なビデオ制作会社が、マドリードの街頭で高齢者を撮影した数時間分の映像を収録し終えたばかりです。どのような条件であれば、ドキュメンタリーに使用する画像を使用するすべての人から同意を得る必要がないのでしょうか?
A. 同意を得ることが現地の法律によって任意であるとみなされる場合。
B. 企業がドキュメンタリープロバイダーとしての地位により正当な利益を主張できる場合。
C. 同意を得るのに過度の労力がかかると判断された場合。
D. 企業が映像を法定年齢に達したデータ主体のみに限定している場合。
Answer: (解答を表示する**)**
GDPRによると、同意は個人データ処理の6つの法的根拠の一つですが、唯一の根拠ではありません。他の5つは、契約、法的義務、重要な利益、公的任務、そして正当な利益です。
正当な利益は、個人データを自社の利益または第三者の利益のために処理する管理者によって主張することができます。ただし、そのような処理がデータ主体（特に未成年者）の権利と自由を侵害しない限りにおいてです。GDPRはまた、ジャーナリズム目的、または学術的、芸術的、文学的表現の目的で個人データを処理することが、表現の自由および情報の自由という正当な利益の行使に必要となる場合があることも認めています。したがって、企業は、ジャーナリズム、芸術的、文学的表現の目的のために処理が必要であること、そしてデータ主体の合理的な期待とプライバシーへの潜在的な影響を考慮していることを実証できる場合、ドキュメンタリーに使用する画像のすべての所有者から同意を得る必要がない可能性があります。企業はまた、そのような処理に適用される可能性のある関連する国内法または行動規範を遵守する必要があります。参考文献：
* GDPR第6条(1)(a)-(f)
* GDPR、序文47
* GDPR第85条

最新問題: **163**
欧州データ保護指令 95/46/EC の目的は何でしたか?
A. 欧州人権条約の実施をすべての加盟国間で調和させること。
B. プライバシーの保護と個人データの国境を越えた流れに関する OECD ガイドラインを実施する。
C. 個人データが欧州連合外に転送されるのを完全に防止します。
D. 個人の基本的権利の保護と、加盟国間でのデータの自由な流れをさらに調和させる。
Answer: D (メーッセージを残す**)**
欧州データ保護指令95/46/ECの目的は、欧州連合（EU）域内における個人データ保護のための共通の法的枠組みを確立し、域内市場における個人データの自由な移動を確保することであった。この指令は、個人データの処理が個人の基本的権利と自由、特にプライ

バシー権に影響を与え、これらの権利は尊重され、保護される必要があるという認識に基づいている。同時に、この指令は、個人データの自由な流通がEUの経済的 -社会的発展に不可欠であり、データ保護法の調和が加盟国間の情報交換とサービス提供を促進することを認識していた。したがって、この指令は、個人データ処理に関する主要な原則、義務、権利を規定し、各国のデータ保護当局間の協力と調整のためのメカニズムを提供することにより、個人の権利の保護と域内市場の促進のバランスをとることを目指した。参照 :1995年10月24日の欧州議会及び理事会指令95/46/EC 個人データの処理に関する個人の保護及び当該データの自由な移動に関するもの」、データ保護指令 - Wikipedia

最新問題**: 164**
GDPRでは、管理者に対し、データ主体に対し、データの処理に関する詳細な情報を提供することが義務付けられています。a. 管理者がデータ主体から直接データを取得する場合、以下の情報のうち、法的に提供する必要がないものはどれですか？
A. 受信者または受信者のカテゴリ。
B. 関係する個人データのカテゴリ。
C. アクセス、消去、制限、移植性の権利。
D. 監督機関に苦情を申し立てる権利。
Answer: (解答を表示する**)**
GDPR第13条によれば、管理者がデータ主体から直接個人データを取得する場合、管理者はデータ主体に対し、データ処理に関する一定の情報（管理者の身元および連絡先、処理の目的および法的根拠、受領者または受領者の区分、保管期間、データ主体の権利、苦情申し立て権など）を提供しなければなりません。ただし、データ主体は自らデータを提供したため、これらの情報は既に把握しているため、管理者はデータ主体に個人データの区分を提供する必要はありません。これは、管理者がデータ主体以外の情報源から個人データを取得する場合に適用される第14条とは異なり、管理者はデータ主体に対し、個人データの区分とデータの情報源を通知する必要があります。参考：
GDPR 第13条 - データ主体から個人データを収集する場合に提供される情報 GDPR 第14条 - データ主体から個人データを取得しない場合に提供される情報 第13条: データ主体から個人データを収集する場合に提供される情報 - GDPR

最新問題**: 165**
欧州連合 (EU) 加盟国で個人データを収集する場合、企業がデータ主体以外のソースから個人データを収集するには、何をする必要がありますか?
A. ソースのセキュリティに合わせてセキュリティをアップグレードします
B. 対象者にコレクションについて通知する
C. 適切な時間内にデータを更新する
D. データに関する公的な通知を提供する
Answer: B (メーッセージを残す**)**

最新問題**: 166**
GDPR では、データ主体の知らないうちにまたは同意なしに、データ主体の機密性の高い医療情報を収集、使用、開示することが最も許可されないのは誰でしょうか?
A. データ主体に関わる、またはデータ主体の健康に関する法的紛争の裁定に関与する司法関係者。
B. 公衆衛生を担当する公的機関であり、一般大衆の保護のためにそのような情報を共有することが必要であると考えられる場合。
C. データ主体の医療に携わる医療専門家で、データ主体の生命がそのような情報のタイムリーな伝達に左右される場合。

D. 問題となっている病状に関連する記事を執筆しているジャーナリストで、そのような情報の公表は公共の利益になると考えている人物。
Answer: (解答を表示する**)**
参考 :https://www.eui.eu/Documents/ServicesAdmin/DeanOfStudies/ResearchEthics/Guide-Data-Protection-Research.pdf

最新問題**: 167**
ある団体のウェブサイトは、EUユーザーのパソコンおよびモバイルデバイスのブラウザにテキストファイルを保存します。その前に、当該団体は、以下のどの枠組みに基づいて、情報と同意を含む通知をユーザーに提供する必要がありますか？
A. 電子プライバシー指令 2002/58/EC。
B. 電子商取引指令 2000/31/EC。
C. 一般データ保護規則 2016/679。
D. データ保護指令 95/46/EC。
Answer: D (メーッセージを残す**)**

最新問題**: 168**
EU 法に基づく権利の行使を希望する個人の行動について決定を下すのはどの司法機関ですか?
A. 欧州連合司法裁判所
B. 欧州データ保護委員会
C. 会計検査院
D. 欧州人権裁判所
Answer: (解答を表示する**)**

最新問題**: 169**
シナリオ
次の質問に答えるには、以下を使用してください。
アウトライアーズ社は、ここ数年で大幅な収益減少に見舞われている旅行サービス会社です。新任マネージャーのジョナサンは、その一因として会社のウェブサイトの老朽化が考えられます。調査を行った後、彼は新興IT企業ZenFiTechの営業担当者と面談し、アウトライアーズの経営難に陥っている事業のために、最先端のウェブサイトを新たにデザインしてくれることを期待します。
交渉中、ZenFiTechの担当者は、詳細なアンケートを通じて顧客情報を収集する計画について説明しました。このアンケートは、特定の旅行先に合わせて顧客の好みをカスタマイズするために活用できます。Outliers Inc.は、年齢、収入、民族など、目標達成に最も役立つデータカテゴリーをいくつでも選択できます。ジョナサンはこのアイデアに感銘を受けましたが、アンケートでは顧客からデータ収集への明示的な同意が必要となるため、このアプローチの成功度を測定する方法も必要だと考えています。ZenFiTechの担当者は、顧客がどのようにウェブサイトを利用しているかをより深く理解するために、新しいウェブサイトのトラフィックを分析するプ

ログラムも実行することを提案しました。彼は、顧客のデバイスに複数のCookieを配置する計画について説明します。これらのCookieにより、同社はIPアドレスやその他の情報を収集できます。例えば、顧客がどのサイトからアクセスしたか、Outliers Inc.のウェブサイトで過ごした時間、どのページを訪問したかなどです。これらの情報はすべてログファイルにまとめられ、ZenFiTechは特別なプログラムを使って分析します。Outliers Inc.は、ウェブサイトの効果を評価するために集計統計情報を受け取りたいと考えていました。ジョナサンはZenFiTechにこれらのサービスを熱心に依頼しています。
Outliers Inc. のウェブサイト Cookie の使用に関して、正しい記述は次のうちどれですか?
A. ZenFiTech は Cookie から収集されたデータの集計統計のみを受信するため、追加の同意は必要ありません。
B. Outliers Inc. から要求されたサービスの使用を有効にするためにすべての Cookie が厳密に必要というわけではないため、Cookie の使用には同意要件が適用されます。
C. クッキーを使用すると位置情報が追跡される可能性があるため、顧客から明示的な同意を得る必要があります。
D. 関係するデータのカテゴリのため、Cookie の使用に関する明示的な同意を顧客から別途取得する必要があります。
Answer: D (メーッセージを残す**)**

最新問題**: 170**
データ侵害が発生した場合、データ管理者が監督当局またはデータ主体に提供する必要がない情報の種類はどれですか?
A. 侵害の予測される結果。
B. 違反に対処するために講じられている対策。
C. データを保護するために使用されるセキュリティ保護手段の種類。
D. 適切なデータ保護責任者の連絡先の詳細。
Answer: (解答を表示する**)**
CIPP/E 学習ガイドによると、GDPR の第 33 条では、データ管理者は、個人データの漏洩が自然人の権利と自由にリスクをもたらす可能性が低い場合を除き、過度の遅延なく、可能であれば、漏洩を認識してから 72 時間以内に監督機関に通知する必要があります。1GDPR の第 34 条では、データ管理者は、漏洩が自然人の権利と自由に高いリスクをもたらす可能性がある場合、過度の遅延なく、個人データの漏洩をデータ主体に伝える必要があります 2。両条項では、データ管理者が監督機関とデータ主体に提供する必要がある最低限の情報が規定されており、これには、漏洩の性質、関係するデータ主体と個人データ記録のカテゴリと概数、データ保護責任者またはその他の連絡先担当者の名前と連絡先、漏洩の可能性のある結果、および漏洩に対処してその悪影響を軽減するために講じられた、または提案された措置が含まれます12。しかし、どちらの条項も、データ管理者がデータ保護に用いるセキュリティ対策の種類を開示することを義務付けていない。この情報は通知の目的とは無関係であり、データのセキュリティをさらに損なう可能性もあるためである3。参考文献 :1 :CIPP/E学習ガイド、84ページ ;GDPR第33条 ;データ漏洩通知に関する事例に関するガイドライン01/20212 :CIPP/E学習ガイド、85ページ ;[GDPR第34条] ;ガイドライン01
/2021 データ侵害通知に関する例3: 個人データ侵害 | 欧州データ保護監督官; データ侵害とは何か、そして私たちは何をしなければならないのか... - 欧州委員会。

最新問題**: 171**
シナリオ
次の質問に答えるには、以下を使用してください。
Zandelay Fashion（以下Zandelay」）は、アイルランドのダブリンに本社を置き、約650人の従業員を擁する、国際的なオンライン衣料品小売業者です。マーティンは最近任命されたデータ保護責任者であり、一般データ保護規則（GDPR）およびその他のプライバシー法の遵守を監督しています。

同社は、子供を含むあらゆる年齢層を対象に、男性用と女性用の衣料品ラインを提供しています。その過程で、顧客の嗜好やクレジットカード番号や銀行口座番号といった機密性の高い金融情報など、大量の顧客情報を処理しています。
収益成長を積極的に図るため、CEOのジェリーはマーティンに対し、顧客の購入履歴を分析し、プロファイリングに重点を置いた新しいモバイルアプリとロイヤルティプログラムを導入することを伝えました。マーティンはCEOに対し、(a) こうした活動に伴う潜在的なリスクを考慮すると、ザンデレイ社はこの新しい取り組みとそのプライバシーへの影響を評価するためにデータ保護影響評価を実施する必要があること、(b) この評価結果から、適切な保護措置を講じない場合に高いリスクが生じる可能性があることを示唆しました。ザンデレイ社は、アプリとロイヤルティプログラムを導入する前に、アイルランドのデータ保護コミッショナーとの事前協議を行う必要があるかもしれません。
ジェリーはマーティンに対し、監督当局と直接交渉し、ザンデレイの事業計画と関連する処理活動の詳細を開示しなければならない可能性について不満を述べている。
事前協議の際に、Zandelay は監督当局に何を提供する必要がありますか?
A. 顧客が意図したプロファイリング活動に明示的に同意したことを示す記録。
B. 意図した処理の複雑さの評価。
C. Martin の専門的な資質とデータ保護法に関する専門知識を証明する証明書。
D. 意図された処理の目的と手段。
Answer: D (メーッセージを残す**)**

最新問題**: 172**
シナリオ
次の質問に答えるには、以下を使用してください。
Wonderkidsは、託児サービスのオンライン予約サービスを提供しています。Wonderkidsはフランスに拠点を置いていますが、ウェブサイトはスイスの企業を通じて運営されています。サービスの一環として、Wonderkidsは、提供されたすべての個人データを、自社のシステムを通じて予約された託児サービス提供者に提供します。ウェブサイトで収集される個人データの種類には、託児サービスを予約した人の氏名、住所、連絡先、そして保育を受ける子供の氏名、年齢、性別、健康情報が含まれます。Wonderkidsのウェブサイトのプライバシーに関する声明には、次のように記載されています。
WonderkKidsは、本ウェブサイトを通じてお客様からご提供いただいた情報を、スケジュール管理および健康 ·安全上の理由から、お客様の保育事業者に提供します。また、お客様およびお子様の個人情報を当社の正当な事業目的で使用する場合もあります。また、データの保管にはスイスに所在する第三者ウェブサイトホスティング会社を利用しています。スイスにある機器に保管されるデータは、お客様およびお子様の個人情報の適切な保護を保証するための欧州委員会の規定を満たしています。お客様およびお子様の個人情報は、お客様にとって真に価値のある企業とのみ共有されます。個人情報をご提供いただくことで、お客様は関連企業への情報提供およびプロモーション情報の送付に同意するものとします。
当社は、お客様とお客様のお子様の個人情報を最長 28 日間保持することがあります。その時点でデータは匿名化されます。ただし、お客様の個人情報が 28 日を超えて正当な事業目的で使用される場合は、最長 2 年間保持されることがあります。
当社は、お客様とお子様の個人情報をお客様の同意を得て処理しております。特定の情報をご提供いただけない場合、当社のサービスをご利用いただけない場合があります。お客様には、お客様とお子様の個人情報へのアクセスを要求する権利、お客様とお子様の個人情報を訂正または消去する権利、お客様とお子様の個人情報の訂正または消去を求める権利、お客様とお子様の個人情報の処理に異議を申し立てる権利があります。また、当社のデータ処理活動について監督当局に苦情を申し立てる権利もあります。Wonderkidsはプライバシーステートメントにおいて、どのような追加情報を提供する必要がありますか？
A. データを保護するための技術的および組織的な対策。

B. データが共有される受信者のカテゴリ。
C. ホスティング会社の連絡先情報。
D. プロモーション メールを送信する頻度。
Answer: B (メーッセージを残す**)**

最新問題**: 173**
シナリオ
次の質問に答えるには、以下を使用してください。
ジョーは、DNA鑑定サービスを提供するカナダ企業Who-RUの新しいプライバシーマネージャーです。本社はモントリオールにあり、従業員全員がそこに勤務しています。同社はカナダ人のみにサービスを提供しています。ウェブサイトは英語とフランス語で提供され、カナダの通貨のみを受け付け、カナダ国外からのインターネットトラフィックをブロックしています ただし、この対策でカナダ国外からのトラフィックをすべてブロックできるわけではありません）。また、DNAレポートをカナダ国外に送付するよう要求する注文は処理せず、カナダ国外の返送先住所が記載されている注文は返品されます。
Who-RU の社長ボブ氏は、EU でこの製品に対する関心が非常に高いと考えており、同社は顧客基盤を拡大するためのさまざまな計画を検討しています。
最初の計画は、共同でWe-Track-Uと名付けられ、アプリを用いて既存のカナダの顧客基盤に関する情報を収集します。この拡張により、カナダの顧客は海外旅行中にアプリを使用できるようになります。ボブは、このアプリを用いて位置情報の収集を行うことを提案します。この計画が有望であれば、ボブはプッシュ通知とテキストメッセージを用いて既存顧客にEU版サービスの事前登録を促すことを提案します。ボブはこの作業計画をWe-Text-Uと呼んでいます。十分な事前登録数を集めた後、EU向けのコンテンツとサービスを開発する予定です。
もう1つのプランは Customer for Life」と呼ばれる。これは、同社のアプリを通じて、DNA情報の保存や、他のアプリや医療機関との共有といった追加サービスを提供するという構想だ。同社の契約書には、顧客のDNAを無期限に保管し、新サービスの提供や顧客へのマーケティングに活用できることが明記されている。また、顧客はダイレクトマーケティングへの同意を撤回しないことに同意する、と明記されている。マーケティングディレクターのポール氏は、同社がこれらの条項を最大限に活用し、契約によって同意が無効となるため、顧客が同意を撤回しようとしても回避できると提案している。
最終計画は、EUにおけるブランドプレゼンスの構築です。同社はすでにこのプロセスに着手しており、ドイツにあるビルの命名権を購入する手続きを進めています。このビルには、Who-RUの幹部が海外旅行中に利用できるオフィススペースがいくつか設けられる予定です。このオフィスにはテクノロジーやインフラ設備は一切なく、机と椅子がいくつか置かれただけのシンプルな部屋です。
命名権契約に関する最近の出張中、ボブのノートパソコンが盗まれました。ノートパソコンには、Who-RUの顧客5,000人（全員カナダ在住）の暗号化されていないDNAレポートが保存されていました。レポートには、顧客名、生年月日、民族、人種的背景、親族名、性別、そして時折健康情報も含まれていました。
Who-RU がアプリを使用して位置を追跡することに決めた場合、GDPR に準拠するために何をする必要がありますか?
A. アプリユーザーから同意を得ます。
B. ユーザーに透明な通知を提供します。
C. データを匿名化し、遅延を追加して、リアルタイムの位置情報が公開されないようにします。
D. 位置データは個人データの特別なカテゴリであるため、裁判所命令を取得します。
Answer: A (メーッセージを残す**)**
GDPRによると、位置データは個人の習慣、嗜好、行動に関する情報を明らかにする可能性のある個人データの一種です1。また、位置データは、個人の健康状態、民族的出身、宗教的信念に関する情報を明らかにする場合、個人データの特別なカテゴリーとみなさ

れることもあります2。したがって、位置データは、同意、契約、法的義務、重要な利益、公共の利益、正当な利益など、有効な法的根拠を必要とするGDPRの個人データの合法的処理に関する規則の対象となります2。
このシナリオでは、Who-RUは自社のアプリを用いて位置情報を追跡することを決定しました。これは、アプリユーザーから位置情報データを収集・処理することを意味します。このデータは、アプリユーザーを特定するために利用されるだけでなく、ユーザーの興味、嗜好、行動に関する情報を推測するためにも使用されます。したがって、Who-RUはEU2諸国における個人の行動を監視しているため、カナダ国民のみにサービスを提供している場合でも、GDPRを遵守する必要があります。
位置データ処理の法的根拠の一つとして考えられるのは同意です。これは、アプリユーザーが位置情報データの収集と利用について、十分な情報に基づいた、具体的かつ自由な同意を与える必要があることを意味します2。同意は処理開始前に取得する必要があり、いつでも容易に撤回できる必要があります2。また、同意はきめ細やかでなければならないため、アプリユーザーは位置情報データの共有目的と種類を選択できる必要があります1。
したがって、Who-RU がアプリを使用して位置を追跡することを決定した場合、アプリユーザーから同意を取得し、位置データが処理される方法、理由、期間、データにアクセスできるユーザー、GDPR の下でのユーザーの権利について明確で透明性のある情報を提供しなければなりません12。Who-RU はまた、同意が自発的であること、およびアプリユーザーがアプリの機能や品質に影響を与えることなく、位置追跡をオプトアウトできることを保証する必要があります12。参照: 1 政策概要: 既存のプライバシー法に基づく位置データ | FPF。5 で入手可能 (アクセス日: 2023 年 12 月 11 日)2 一般データ保護規則 (GDPR) とは何ですか? | Cloudflare。6 で入手可能 (アクセス日: 2023 年 12 月 11 日)

最新問題: **174**
ほとんどのプロセッサーがデータ処理活動に関連して保持しなければならない記録に含める必要がないのは次のどれですか?
A. プロセッサが代理を務める各コントローラの名前と連絡先の詳細。
B. プロセッサが機能している各コントローラに代わって実行される処理のカテゴリ。
C. プロセッサが行動している各コントローラに代わって実行される第三国への個人データの転送の詳細。
D. プロセッサが代理を務める各コントローラに代わってプロセッサが実行する処理活動に関連して実施されたデータ保護影響評価の詳細。
Answer: C (メーッセージを残す**)**
参照 https://gdpr-info.eu/art-30-gdpr/

最新問題: **175**
スペインの雇用主が従業員の個人データを毎年国の税務当局に送信する場合、どの GDPR 原則に最も依存するでしょうか?
A. 従業員の同意。
B. 雇用主の法的義務。
C. 行政の正当な利益。
D. 従業員の重大な利益の保護。
Answer: (解答を表示する**)**
GDPR第6条(1)(c)では、管理者が負う法的義務を遵守するために必要な場合には、処理は合法であると規定されています。
スペイン（およびEU全域）の雇用主は、給与・税務データを各国の税務当局に提出する法的義務を負っています。この義務は、同意（A）（実質的な選択肢がないため無効）、正当な利益（C）、または生命に関わる利益（D）に依拠することはできません。
したがって、正しい根拠は法的義務（B）です。
#参照:GDPR第6条(1)(c)、CIPP/E教科書(第3版)、第7章「合法的な処理基準」。

最新問題: **176**
データ保護の分野における最初の法的拘束力のある国際文書は次のどれですか?
A. 世界人権宣言。
B. 一般データ保護規則。
C. プライバシーと電子通信に関する EU 指令。
D. 条約 108。
Answer: D (メーッセージを残す**)**

最新問題: **177**
X社は給与計算データの処理をプロバイダーY社に委託しています。プロバイダーY社は、この暗号化されたデータを自社のサーバーに保存しています。プロバイダーY社のIT部門は、誰かがシステムに侵入し、サーバーからデータのコピーを持ち出したことを知りました。このような場合、プロバイダーY社は誰に通知する義務があるでしょうか？
A. 一般の人々
B. X社
C. 法執行機関
D. 監督機関
Answer: B (メーッセージを残す**)**
GDPR第33条によれば、個人データの漏洩が発生した場合、処理者（プロバイダーY）は漏洩を認識した後、遅滞なく管理者（企業）に通知するものとします。処理者は、法律で別途義務付けられている場合を除き、監督当局、一般市民、または法執行機関に通知する義務を負いません。管理者は、漏洩がデータ主体の権利と自由にリスクをもたらす可能性が低い場合を除き、監督当局および必要に応じてデータ主体に通知する責任を負います。参考：
GDPR の第 33 条は、個人データ侵害の監督機関への通知を規制しています。
[GDPR第34条]は、個人データ侵害に関するデータ主体への通知を規制しています。
データ侵害通知に関する管理者と処理者の役割と責任を説明する ICO ガイダンス。

最新問題: **178**
WP29の「規則2016/679に基づく個人データ漏洩通知に関するガイドライン」では、データ漏洩を透明性を持って伝える方法の例が示されています。データ主体への漏洩通知に効果的ではない方法として挙げられているのは次のうちどれですか？
A. 企業ブログのお知らせ
B. 郵便通知
C. 直接的な電子メッセージ
D. 印刷メディアで目立つ広告
Answer: A (メーッセージを残す**)**

最新問題: **179**
ノートブックやハードコピー ファイルに含まれる情報など、物理的な形で存在する個人データにはどのような状況で GDPR が適用されますか?
A. 個人データが、印刷、ラベル付け、スタンプなどの特定の自動処理活動の物理的な出力として生成される場合のみ。
B. 個人データが画像スキャンや光学式文字認識などの特定のコンピュータ処理の対象となる場合のみ。

C. 個人データが、コンピュータによる配布やファイリングなど、何らかの方法で自動化された手段によって処理される場合のみ。
D. 個人データが、ファイリング システムの一部を形成するように十分に構造化された方法で処理される場合のみ。
Answer: D (メーッセージを残す**)**
参考 :https://www.zimmerslaw.com/english-1/data-protection/

最新問題**: 180**
企業が契約ルートに基づいて国際データ転送を行うことを選択した場合、次のどれが有効な標準契約条項のセットではないでしょうか?
A. 決定 2001/497/EC (EU 管理者から非 EU または EEA 管理者へ)。
B. 決定 2004/915/EC (EU 管理者から非 EU または EEA 管理者へ)。
C. 決定 2007/72/EC (EU プロセッサから非 EU または EEA コントローラへ)。
D. 決定 2010/87/EU (EU コントローラーからの非 EU または EEA プロセッサー)。
Answer: C (メーッセージを残す**)**
これは、GDPRまたは以前のデータ保護指令95/46に基づき欧州委員会が採択した決定のいずれにも該当しないため、有効な標準契約条項集ではありません。EU域内の処理者からEU域外またはEEA域内の管理者への適切な決定は、決定2010/87/EUであり、これは決定2004/915/ECによって改正されました。決定2007/72/ECは、実際にはスイスにおける個人データ保護の適切性の認定に関連しています。参考資料：
* 無料のCIPP/E学習ガイド、18ページ、セクション3.4.2
* 国際送金に関する標準契約条項、第1.1項
* 標準契約条項（SCC）第2.1条
* 決定2007/72/EC

最新問題**: 181**
データ管理者はデータ保護責任者を任命します。以下の条件のうち、GDPR第37条から第39条に違反しないものはどれですか？
A. データ保護責任者が ISO 27001 監査人認定を持っていない場合。
B. データ保護責任者がデータ処理者によって提供される場合。
C. データ保護責任者がマーケティング予算も管理している場合。
D. データ保護責任者がデータ管理者から指示を受けた場合。
Answer: A (メーッセージを残す**)**
参照：
ISO 27001 監査人認証を受けていないデータ保護責任者をデータ管理者が任命しても、GDPR 第 37 条から第 39 条の違反にはなりません。GDPR 第 37 条 (5) によれば、データ保護責任者は専門的な資質、特にデータ保護法と慣行に関する専門知識、および第 39 条で言及されているタスクを遂行する能力に基づいて任命される必要があります 1。ただし、GDPR では、データ保護責任者が備えていなければならない正式な資格や認証を規定しておらず、データ処理活動の複雑さと機密性に応じて、管理者または処理者の裁量で必要な専門知識のレベルを決定できます 2。したがって、情報セキュリティ管理システムの標準である ISO 27001 監査人認証を受けていないからといって、必ずしもデータ保護責任者がその役割に対して資格や能力がないということにはなりません。
その他の選択肢は、GDPR第37条から第39条に違反するため、正しくありません。GDPR第37条 (6)によれば、データ保護責任者は管理者または処理者の職員であってもよく、また、サービス契約に基づいて業務を遂行してもよいとされています1。ただし、データ保護責任者は独立性を保ち、管理者または処理者の最高経営責任者に直接報告する必要があります3。したがって、データ保護責任者が

データ処理者によって提供される場合、利益相反や自律性の欠如が生じる可能性があり、GDPR第38条（3）および（6）に違反する可能性があります4。
GDPR第38条(6)によれば、データ保護責任者は利益相反を招かない限りにおいて、他の業務や義務を遂行することができる4。しかし、マーケティング予算の管理は利益相反を伴う可能性が高い。なぜなら、データ保護責任者はマーケティングに関連するデータ処理活動を監督し、助言する必要があり、それがデータ保護責任者としての役割と両立しない可能性があるからである5。したがって、データ保護責任者がマーケティング予算も管理する場合、GDPR第38条(6)に違反することになる4。
GDPR第38条(3)によれば、データ保護責任者は、その職務の遂行に関していかなる指示も受けてはならないとされている4。データ保護責任者は、管理者または処理者および従業員への通知と助言、コンプライアンスの監視、監督機関への協力、データ主体と監督機関の連絡窓口としての役割など、GDPRで割り当てられた職務を独立して遂行しなければならない6。したがって、データ保護責任者がデータ管理者から指示を受けた場合、GDPR第38条(3)に違反することになる4。参考文献：1：GDPR第37条 2：データ保護責任者（DPO）に関するガイドライン 3：GDPR第38条(2) 4：GDPR第38条 5：データ保護責任者（DPO）｜欧州委員会6：GDPR第39条

最新問題: **182**
WP29の「規則2016/679に基づく個人データ漏洩通知に関するガイドライン」では、データ漏洩を透明性を持って伝える方法の例が示されています。データ主体への漏洩通知に効果的ではない方法として挙げられているのは次のうちどれですか？
A. 郵便通知
B. 直接的な電子メッセージ
C. 企業ブログのお知らせ
D. 印刷メディアで目立つ広告
Answer: C (メーッセージを残す**)**
WP29の「規則2016/679に基づく個人データ漏洩通知に関するガイドライン」によれば、個人データ漏洩に関するデータ主体への通知は、明確、簡潔、透明性があり、容易にアクセスでき理解しやすいもので、明瞭で平易な言葉を用いるべきである。また、通知は合理的に可能な限り速やかに、監督当局と緊密に協力して行うべきである。ガイドラインでは、データ主体への漏洩通知に効果的な方法の例がいくつか示されている。例えば、直接的な電子メッセージ（電子メール、SMS、ダイレクトメッセージなど）、郵送による通知、印刷媒体における目立つ広告、影響を受けるウェブサイトのホームページへの通知などである。しかし、ガイドラインでは、企業ブログやソーシャルメディアへの通知は、影響を受けるすべてのデータ主体に届かず、データ主体が自主的な保護措置を迅速に講じることができないため、効果的な通知方法ではないとも述べられている。
したがって正解はCです。企業ブログでのお知らせです。参考文献：
* WP29の「規則2016/679に基づく個人データ漏洩通知に関するガイドライン」、20～211ページ

最新問題: **183**
英国は、ブレグジットの規定に基づきEUを離脱した後、十分性認定を求めることになります。その理由は何ですか？

A. 加盟国が EU を離脱すると、適格性の決定は自動的に失効します。
B. 英国はEUに加盟していないため、信頼性が低下しています。
C. 保険長官は、データ保護法により適切性の判断が必要であると判断しました。
D. 英国は GDPR の対象外となったため、第三国となりました。
Answer: D (メーッセージを残す**)**

最新問題**: 184**
Planet 49 CJEU の判決では、事前にチェックを入れたボックスの問題についてどのような判決が出ましたか?
A. いかなる状況においても有効な同意とはなりません。
B. 技術的に必要であると判断された場合は許可されます。
C. 処理活動の記録簿に記録されている場合は許可されます。
D. 処理が正当な利益の目的のために必要な場合、有効な同意を構成します。
Answer: A (メーッセージを残す**)**

最新問題**: 185**
EU 非加盟国のデータ保護レベルの適切性を確認する調査結果を採用する権限を持つ機関はどれですか?
A. 欧州議会
B. 欧州委員会
C. 第29条作業部会
D. 欧州理事会
Answer: (解答を表示する**)**
GDPR第45条に基づき、欧州委員会は、評価に基づき、EU域外の国、EU域内の地域もしくはセクター、または国際機関が適切なレベルのデータ保護を確保しているかどうかを判断する権限を有します。これは、当該国または組織のデータ保護規則および基準がEUのものと同等であることを意味します。適切性認定の結果、個人データはEU域内から当該国または組織へ、追加の保護措置や承認なしに自由に流通できるようになります。欧州委員会は、日本、カナダ、EU-米国データプライバシーフレームワークなど、複数の国や組織に対して適切性認定を採択しています。参考文献 :EU域外諸国のデータ保護の適切性、適切な保護レベル

最新問題**: 186**
シナリオ
次の質問に答えるには、以下を使用してください。
サンディは最近、2016年に設立された広告テクノロジー企業Market4Uにプライバシーおよびデータガバナンス担当バイスプレジデントとして入社しました。データインベントリの実施という最初の取り組みを通して、サンディはMarket4Uが設立以来収集してきた1,900万人のグローバル連絡先リストを保有していることを知りました。膨大なデータ量のリスクを認識していたサンディは、2018年5月以前にMarket4Uのシステムに入力された連絡先のうち、Market4Uのコンテンツに最近アクセスした連絡先を除いて、すべて削除したいと考えていました。しかし、営業担当バイスプレジデントのダンは、すべての連絡先がMarket4Uのクライアントにとって、成功したマーケティングキャンペーンや業界動向に関する有用な情報を提供しているとサンディに伝えました。
ダンはサンディに、スポーツ -エンターテイメント業界の顧客獲得に注力したいと伝えました。この顧客獲得を支援するため、Market4Uのマーケティングチームは、Market4Uのウェブサイトフォームに、ホワイトペーパーのダウンロード、Market4U

フォーラムへの参加用アカウント作成、イベントへの参加など、いくつかの新しいフィールドを追加することにしました。これらのフィールドには、生年月日や給与などが含まれています。
Market4U のリスクを最小限に抑えながら、サンディがダンが求める洞察を得るための最善の方法は何でしょうか?
A. 匿名化された個人データのみを分析します。
B. 仮名化された個人データのみを分析します。
C. 傾向分析を実施した後、2018 年 5 月以前に収集されたすべてのデータを削除します。
D. 第三者に分析を依頼し、Market4U のシステムからデータを削除します。
Answer: (解答を表示する**)**
GDPR によると、仮名化とは、データセット内の個人を識別する情報を置き換えたり削除したりする手法です。仮名化されたデータは、追加情報を使用しない限り、特定のデータ主体に帰属させることができなくなります。追加情報は別途保管され、帰属不可を保証するための技術的および組織的措置の対象となります1。仮名化は匿名化の方法ではありません。匿名化とは、データが不可逆的に変更され、データ主体を識別できなくなることを意味します2。仮名化されたデータは依然として個人データとみなされ、GDPR の対象となりますが、互換性のある目的での追加処理の可能性、一部のデータ主体の権利の免除、データ転送の円滑化など、規則の一部が緩和されています3。
このシナリオでは、Market4Uは広告テクノロジー企業であり、生年月日や給与などの機密データを含む大量の個人データを収集・処理しています。これらのデータは、潜在顧客の嗜好や行動に関する洞察を得るため、また様々な業界におけるトレンドやビジネスチャンスを特定するために活用できます。しかしながら、このデータはMarket4Uにとって、データ漏洩、コンプライアンス違反、風評被害、法的責任といった重大なリスクももたらします。そのため、Market4Uはデータ最小化の原則を適用する必要があります。つまり、目的に必要かつ関連性のあるデータのみを収集・処理し、不要になったデータは削除する必要があります4。
Market4Uがデータ最小化を実現する方法の一つとして、分析に使用する個人データを仮名化することが挙げられます。これにより、Market4Uは個人データ処理に伴うリスクを軽減しつつ、データの有用性と価値をその目的のために維持することができます。仮名化は、Market4Uが目的の限定、保存期間の制限、完全性と機密性といったGDPRのその他の原則を遵守する上でも役立ちます5。また、仮名化により、Market4Uは、データ主体の権利と利益を尊重する限りにおいて、分析のための個人データ処理の法的根拠として正当な利益に依拠することが可能になります6。
したがって、Market4Uのリスクを最小限に抑えながら、サンディがダンが求める洞察を得るための最善の方法は、仮名化された個人データのみを対象に分析を行うことです。これにより、Market4Uはデータ主体のプライバシーとセキュリティを損なうことなく、正当な事業目的のためにデータを利用できるようになります。
その他のオプションは、次の理由により正しくありません。
* A. 匿名化された個人データのみを用いて分析を行うことは、Market4Uにとって実現可能でも効果的でもありません。匿名化は非常に困難で複雑なプロセスであり、個人を直接的または間接的に特定できるあらゆる情報を削除または改変する必要があるためです。また、匿名化はデータの正確性、品質、有用性を損なう可能性があり、分析の価値と目的を損なう可能性があります。さらに、匿名化は不可逆的であるため、Market4Uは必要に応じて元のデータを復元することができません2。
* C. 傾向分析を実施した後、2018 年 5 月以前に収集されたすべてのデータを削除すると、個人データは処理目的に必要な期間のみ保持する必要があることを要求する保存制限の原則に違反するため、GDPR に準拠しません。
Market4Uは、特にデータが古かったり、関連性がなかったり、過剰であったりする場合、必要以上に長期間データを保持することを正当化できません。さらに、分析後にデータを削除しても、データ漏洩や不正アクセスなど、データ処理に伴うリスクを排除することはできません4。

* D. 分析を実施し、Market4U のシステムからデータを削除するために第三者を調達することは、個人データを別のデータ管理者またはデータ処理者に転送することになり、GDPR に基づく追加の保護措置と義務が必要になるため、Market4U にとって良い解決策ではありません。
Market4Uは依然としてデータのコンプライアンスとセキュリティの確保に責任を負い、第三者とデータ処理契約を締結し、必要に応じてデータ主体に通知し、同意を得る必要があります。さらに、第三者を調達することは、Market4Uにとって、データの管理と可視性の喪失、または第三者による不正または違法な処理へのデータの露出など、追加のコストとリスクを伴います7。
参照: 1 GDPR 第 4 条 (5) 2 匿名化 | ICO23 仮名化 | ICO34 データ最小化 | ICO45 設計およびデフォルトによるデータ保護に関する第 25 条に関するガイドライン 4/2019 | 欧州データ保護委員会56 正当な利益 | ICO67 契約 | ICO7.

最新問題**: 187**
OECDガイドラインの重要な要素の一つは「個人参加原則」です。一般データ保護規則（GDPR）のどの部分がこの原則に最も近いのでしょうか？
A. 第6条から第9条に規定される適法な処理基準
B. 第13条および第14条に規定されている情報要件
C. 第33条および第34条に規定されている違反通知要件
D. 第12条から第22条に基づいてデータ主体に付与される権利
Answer: (解答を表示する**)**
個人参加原則は、公正情報慣行原則（FIPP）の一つであり、法的枠組みの一部ではないものの、現在施行されている多くのデータプライバシー規制で広く採用されています1。FIPPは、個人情報のプライバシーとセキュリティの保護を目的とした公正情報慣行に関するガイドラインです。個人参加原則は、個人には、個人データの訂正または消去を求める権利、個人データにアクセスして確認を得る権利、個人データの使用方法と共有相手について通知を受ける権利、特定の目的に対する同意に異議を唱える権利または同意を撤回する権利など、多くの権利があると定めています2。
一般データ保護規則（GDPR）は、欧州連合（EU）のデータ保護指令を実施するための法的枠組みであり、EU域内のすべての個人の個人データに関する包括的な保護を提供します。GDPRは、個人データへのアクセス、訂正、消去、制限、移転、異議申し立て、個人データに基づく自動化された意思決定の対象とならない権利など、個人に多くの権利を付与しています。これらの権利はFIPP（国際データ保護規則）における権利と類似しており、GDPRの第12条から第22条に記載されています。
したがって、個人参加原則に最も近い規定を提供する GDPR の部分は、第 12 条から第 22 条です。
参考文献:
OECDプライバシー原則
GDPR の 7 つの主要原則は何ですか?
公正情報慣行原則（FIPP）
個人の参加 - 国際プライバシー専門家協会 忘れられる権利とは？ | 消去権 | Cloudflare 一般データ保護規則 - Wikipedia

最新問題**: 188**
すべての必要な条件が満たされていると仮定した場合、欧州委員会に加えて、誰が標準契約条項を採用できますか?
A. 承認されたデータ管理者。
B. 欧州連合理事会。
C. 各国のデータ保護当局。
D. 欧州データ保護監督機関。
Answer: A (メーッセージを残す**)**

説明/参照: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/ standard-contractual-clauses-scc_en

最新問題: **189**
同意の問題に関して、GDPR は加盟国に何に関して選択権を与えているのでしょうか?
A. データ主体が同意を撤回できる期間
B. 沈黙または不活動が同意とみなされる状況
C. 子供が親の同意を得なければならない年齢
D. 同意を伝えるメカニズム
Answer: C (メーッセージを残す**)**

最新問題: **190**
データ保護責任者を任命した後、データ管理者またはデータ処理者にはどのような義務がありますか?
A. データ保護責任者が定義されたタスクの遂行に関して十分な指示を確実に受けられるようにするため。
B. データ保護責任者が、個人の個人データに関する質問に対する唯一の連絡先として機能することを保証します。
C. 組織の慣行を管理し、データ保護の原則への準拠を証明するための行動規範をデータ保護責任者に提出し、承認を得る。
D. データ保護責任者の定義されたタスクを実行し、専門知識を維持するために必要なリソースを提供します。
Answer: C (メーッセージを残す**)**

最新問題: **191**
GDPR の第 30 条に基づき、管理者は以下を除くすべての記録を保持することが義務付けられています。
A. 開示の有無にかかわらず、個人データ漏洩事件。
B. 実施されたデータ インベントリまたはデータ マッピング演習。
C. 個人データが開示された受信者のカテゴリ。
D. 個人データのカテゴリの消去および削除の保持期間。
Answer: (解答を表示する**)**
GDPR第30条は、管理者と処理者に対し、処理活動の記録を保持することを義務付けています。記録には、処理の目的、個人データのカテゴリー、データの受信者、保存期間、セキュリティ対策などの情報が含まれます12。しかし、第30条は、管理者に対し、個人データ漏洩のインシデント（開示の有無にかかわらず）の記録を保持することを義務付けていません。これは、第33条および第34条に基づく別の義務であり、これらの条項では、管理者に対し、個人データ漏洩が自然人の権利と自由にリスクをもたらす可能性が低い場合を除き、監督機関およびデータ主体に個人データ漏洩を通知することを義務付けています34。参考文献 :1 :GDPR第30条 2：英国GDPR第30条に基づき、何を文書化する必要がありますか？ | ICO 3 :GDPR第33条 4 :GDPR第34条 セクション：なし）説明

最新問題: **192**
シナリオ
次の質問に答えるには、以下を使用してください。
Gentle Hedgehog Inc.は、イタリアに設立された民間のウェブサイトデザイン会社です。同社はEU諸国に多数のリモートワーカーを抱えています。最近、Gentle Hedgehogの経営陣は、営業チーム、特にリモートワーカーの生産性が低下していることに気づきました。そこで同社は、欠勤防止、優秀な従業員への報奨、そして営業担当者が顧客と接する際に最高品質のカスタマーサービスを提供することを目的として、堅牢かつプライバシーに配慮したリモート監視システムの導入を計画しています。

ジェントル・ヘッジホッグは最終的に、従業員監視ソフトウェアを提供する中国のベンダー、サウロン・アイ社（欧州本社はドイツ）を雇用しました。サウロン・アイ社のソフトウェアは、コンピューターのカメラやマイク、画面キャプチャ、電子メール、ウェブサイトの履歴、キー入力への24時間365日アクセスを含む強力なリモート監視機能を提供します。ジェントル・ヘッジホッグ本社に安全に設置された中央サーバーから、あらゆるデバイスをリモート監視できます。監視はデフォルトでは非表示ですが、監視とその正確な範囲について、すべてのユーザーに定期的に目立つように通知する、いわゆる透過モードも用意されています。さらに、監視対象の従業員は、ログインするたびに、顔認証を含む組み込みの認証技術を使用する必要があります。
顔認識データを含むすべての監視データは、物理的にはフランスにある Sauron Eye が運営する Microsoft Azure クラウド サーバーに安全に保存されます。
24時間365日のカメラ監視の主な問題は何ですか?
A. 営業時間外および従業員の休日には操作しないでください。
B. モニタリングに同意が必要な第三者を誤って撮影してしまう可能性があります。
C. Gentle Hedgehog のビジネスの文脈で実施される有効な法的根拠はありません。
D. まず労働組合の承認を受け、その後国家 DPA からライセンスを取得する必要があります。
Answer: C (メーッセージを残す)
一般データ保護規則（GDPR）は、職場における従業員の監視を禁止していません。ただし、雇用主は、個人データを処理する際に従業員の権利と自由が保護されるように、特別な規則に従う必要があります。GDPRは、処理がEU内で行われるか否かに関わらず、EU域内に設置された管理者または処理者の活動に関連する個人データの処理に適用されます。また、GDPRは、EU域内に設置されていない管理者または処理者による、EU域内に居住するデータ主体の個人データの処理にも適用されます。この場合、処理活動は、EU域内のデータ主体への商品またはサービスの提供、またはEU域内で行われる限りにおけるその行動の監視に関連しています。
GDPRでは、個人データの処理は合法、公正、かつ透明性があり、規則に定められた6つの法的根拠のいずれかに基づいて行われなければならないと規定されています。従業員監視の最も関連性の高い法的根拠は、雇用主の正当な利益、従業員との契約の履行、または法的義務の遵守です。また、GDPRでは、個人データの処理は、処理の目的に必要な範囲に限定されなければならないこと、そしてデータ主体には、処理の目的と法的根拠、そしてデータ主体の権利とデータ保護のための安全対策について通知されなければならないことも規定されています。
GDPRは、人種や民族的出身、政治的意見、宗教的信念、哲学的信念、労働組合への加入状況を明らかにする生体認証データ、あるいは自然人を一意に識別する目的で処理される生体認証データなど、特別なカテゴリーの個人データの処理に関して、具体的な義務と制限を課しています。これらのデータの処理は、規則に列挙されている10の例外のいずれかに該当する場合を除き、禁止されています。従業員監視に関する最も重要な例外は、データ主体の明示的な同意、雇用、社会保障、社会保障法の分野における管理者またはデータ主体の義務の履行および特定の権利の行使のために必要な場合、または重大な公共の利益のための必要性です。
GDPRは、適切なデータ保護水準が確保されていない第三国または国際機関への個人データの移転に関する規則と要件も定めています。このようなデータの移転は、管理者または処理者が拘束力のある企業準則、標準契約条項、行動規範、認証メカニズムなどの適切な保護措置を講じており、かつデータ主体が執行可能な権利と効果的な法的救済手段を有している場合にのみ許可されます。
このシナリオに基づくと、24時間365日体制のカメラ監視の主な問題は、ジェントル・ヘッジホッグの事業の文脈において、それを実施するための有効な法的根拠がないことです。この選択肢は、以下の理由から、GDPRの原則と要件に最も合致しています。
個人データの処理は、雇用主の正当な利益、従業員との契約の履行、または法的義務の遵守に依拠していないため、正当な法的根拠に基づいていません。従業員が行う仕事の生産性、品質、および安全性を確保するという雇用主の正当な利益は、従業員の権利と自由とバランスが取れていなければなりません。
24時間365日のカメラ監視は、特に業務に関連しない活動やコミュニケーションを対象とする場合、不均衡かつ侵入的となる可能性があります。従業員との契約履行は、24時間365日のカメラ監視を正当化するものではありません。これは、従業員または雇用主の契

約上の義務の履行に必要ではないためです。また、ジェントル・ヘッジホッグの事業において、そのような措置を義務付ける具体的な法律や規制がないため、法的義務の遵守は24時間365日のカメラ監視には適用されません。
監視の目的に必要な範囲に限定されず、カメラやマイクの監視など、従業員の業務の範囲を超えて従業員の私的または個人的な領域に侵入する、過剰で無関係な個人データの収集と処理が含まれます。
The 24/7 camera monitoring is also likely to capture personal data of third parties, such as customers, suppliers or visitors, whose consent is required for the monitoring, and whose rights and freedoms may be affected by the processing.
Is not transparent to the employees, as it does not inform them of the monitoring and its precise scope, and does not give them the opportunity to object or opt out of the monitoring. The monitoring is invisible by default, which means that the employees are not aware of when and how they are being monitored, and what personal data are being collected and processed. The so-called Transparent Mode, which regularly and conspicuously notifies all users about the monitoring and its precise scope, is also insufficient, as it does not provide the employees with a clear and comprehensive information notice, nor with a valid and specific consent form, as required by the GDPR.
Involves the processing of special categories of personal data, such as biometric data or data revealing political opinions or trade union membership, which are not necessary or proportionate for the purposes of the monitoring, and which do not fall under any of the exceptions listed in the regulation. The facial recognition technology used by the monitoring system is a form of biometric data processing, which is prohibited by the GDPR, unless the data subject has given explicit consent, or the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law, or the processing is necessary for reasons of substantial public interest. None of these exceptions apply to the scenario, as the facial recognition technology is not used for any of these purposes, but rather for verifying the identity of the employees each time they log in. The camera and microphone monitoring may also capture personal data revealing political opinions or trade union membership, which are also special categories of personal data, and which are not relevant or proportionate for the purposes of the monitoring.
Involves the transfer of personal data to a third country, such as China, which does not provide an adequate level of data protection, and which may pose additional risks for the rights and freedoms of the employees.
顔認識データを含む監視データは、物理的にはフランスにあるSauron Eyeが運営するMicrosoft Azureクラウドサーバーに安全に保存されます。しかし、Sauron Eyeは従業員監視ソフトウェアを提供する中国のベンダーであり、欧州本社はドイツにあります。つまり、Sauron Eyeは監視データにアクセスしたり、中国の親会社やその他の関連会社に転送したりする可能性があるということです。欧州委員会によると、中国は適切なデータ保護レベルを確保していない第三国です。個人データの中国への転送は、管理者または処理者が拘束的企業準則、標準契約条項、行動規範、認証メカニズムなどの適切な保護措置を提供し、データ主体が執行可能な権利と効果的な法的救済手段を持っている場合にのみ許可されます。しかし、このシナリオではこれらの保護措置や救済手段が実施されていることが示されておらず、したがって中国への個人データの転送はGDPRに違反する可能性があります。
質問に記載されているその他のオプションは、24時間365日のカメラ監視の主な問題ではありません。
GDPRの原則や要件とは直接関係がなく、むしろ加盟国の国内法や規則に関係しており、監視の具体的な状況や状況によって異なる場合があります。GDPRはカメラ監視の運用に正確な期限を定めておらず、処理の性質、範囲、状況、目的、およびデータ主体の権利と自由に対するリスクを考慮した上で、監視の適切な条件と保護手段を決定するのは加盟国の国内法や規則に委ねられています。GDPRはまた、カメラ監視に関して労働組合の承認や国内DPAからのライセンスを要求していませんが、従業員、労働組合、労使協議会、DPA、裁判所などの関係者との協議や関与のための適切な手順やメカニズムを確立するのは加盟国の国内法や規則に委ねられています。
24時間365日のカメラ監視の根本的な問題はそこにあるのではなく、むしろその根本的な問題がもたらす結果や影響、つまり監視の法的根拠が欠如していることにあります。業務時間外や従業員の休暇中にカメラ監視が作動したり、監視に同意が必要な第三者が偶

発的に撮影されたりすることは根本的な問題ではなく、むしろ根本的な問題の結果であり、従業員の業務範囲を超えて、彼らの私生活や個人的な領域にまで踏み込んでくる、過剰かつ不均衡な個人データの収集と処理が問題となっています。労働組合の承認や国家DPAからのライセンスは根本的な問題ではなく、むしろ根本的な問題に対する潜在的な解決策や改善策、つまり監視の透明性と説明責任の欠如、つまり従業員に監視の内容とその正確な範囲が通知されず、監視への異議申し立てやオプトアウトの機会も与えられていないことにあります。
参考文献:
GDPR、第5条、第6条、第7条、第8条、第9条、第10条、第12条、第13条、第14条、第15条、第16条、第17条、第18条、第19条、第20条、第21条、第22条、第23条、第44条、第45条、第46条、第47条、第48条、および第49条。
ビデオ機器による個人データの処理に関するEDPBガイドライン3/2019、5、6、7、8、9、10、11、12ページ
13、そして14。
[GDPRにおける管理者と処理者の概念に関するEDPBガイドライン07/2020]

最新問題**: 193**
一般データ保護規則（GDPR）と欧州評議会条約の両方に当てはまることは何ですか？
108ですか？
A. どちらも個人データの国際転送を規制しています
B. どちらも個人データの手動処理を規定しています
C. どちらも欧州連合諸国にのみ適用されます
D. どちらも、処理活動の監督機関への通知が必要です。
Answer: D (メーッセージを残す**)**
説明/参考: https://rm.coe.int/090000168093b851

最新問題**: 194**
GDPRおよび欧州司法裁判所のSchrems II判決に準拠するため、欧州委員会は、一般的に新しい標準契約条項（SCC）と呼ばれるものを発行しました。その結果、企業は以下のすべてを実施する必要がありますが、次の項目は除きます。
A. SCC に新しい当事者を追加することを明示的に許可する、新しいオプションのドッキング条項を検討してください。
B. 2021 年 9 月 27 日より前に締結され、古い SCC を使用しているすべての契約を、2022 年 12 月 27 日までに新しい SCC に移行します。
C. 企業がデータ輸入者である場合は、2021 年 9 月 27 日時点で新しい SCC を使用して、新しい SCC をサプライ チェーンの関連部分に伝達するための手順を実行します。
D. 英国情報コミッショナー事務局には独自の SCC セットを公開する権限がないため、Brexit 後に英国で新しい SCC を実装します。
Answer: D (メーッセージを残す**)**
一般データ保護規則（GDPR）は、承認された認証に基づき、適切なデータ保護水準を確保していない第三国または国際機関への個人データ移転のためのメカニズムを導入しています。GDPR第46条によれば、適切なデータ保護措置を保証する契約条項は、EUから第三国へのデータ移転の根拠として使用することができます。これには、欧州委員会によって「事前承認」されたモデル契約条項、いわゆる標準契約条項（SCC）が含まれます。
2021年6月4日、欧州委員会は、EU/EEA域内（またはGDPRの適用対象となる）の管理者または処理者からEU/EEA域外（GDPRの適用対象外）に設立された管理者または処理者へのデータ移転について、GDPRに基づく最新の標準契約条項（SCC）を発行しました。こ

れらの最新のSCCは、以前のデータ保護指令95/46に基づいて採択された3セットのSCCに代わるものです。欧州委員会は、SCCの活用に関する実用的なガイダンスを提供し、GDPRに基づくコンプライアンスへの取り組みにおいて関係者を支援するため、質疑応答（Q&A）を作成しました。
Q&A では、企業は以下のすべてを実行する必要があると述べられています。
新たな任意条項であるドッキング条項について考えてみましょう。この条項は、SCCへの新たな当事者の追加を明示的に認めています。Q&Aによると、このドッキング条項により、当初の契約に含まれていなかった管理者および処理者が、後日、データの輸出者または輸入者としてSCCに加入することが可能になります。この条項は、複雑な処理チェーンにおけるSCCの利用を容易にし、複数の契約を締結する必要性を回避できるようにするためのものです。
2021 年 9 月 27 日より前に締結され、古い SCC を使用しているすべての契約を、2022 年 12 月 27 日までに新しい SCC に移行してください。Q&A によると、古い SCC は 2021 年 9 月 27 日に廃止されます。ただし、その日付より前に古い SCC に基づいて締結された契約は、契約の主題である処理操作が変更されず、それらの条項に依拠することで個人データの転送が GDPR の第 46 条 (1) の意味での適切な保護措置の対象となることを保証される場合、2022 年 12 月 27 日まで有効です。2022 年 12 月 27 日以降、古い SCC は第三国へのデータ転送の有効な法的根拠を提供しなくなるため、代わりに新しい SCC を使用する必要があります。
企業がデータ輸入者である場合は、2021年9月27日以降、新しいSCCを用いて、サプライチェーンの関連部署に新しいSCCを浸透させるための措置を講じてください。Q&Aによると、新しいSCCでは、データ輸入者は、SCCに基づいて移転された個人データを処理するすべてのサブプロセッサーと契約を締結し、その契約にSCCに基づいてデータ輸入者に課せられるものと同じデータ保護義務を含めることが求められています。つまり、データ輸入者は、2021年9月27日以降、新しいSCCがサブプロセッサーに浸透していること、およびサブプロセッサーの変更があれば、異議申し立て権を持つデータ輸出者に通知する必要があることを意味します。
Q&A では、企業が以下のことを行わなければならないとは述べられていません。
英国情報コミッショナー事務局には独自のSCCを発行する権限がないため、Brexit後、英国では新しいSCCを導入する必要がある。しかし、これは妥当な記述ではない。英国はEU離脱後も独自のデータ保護体制を有しており、英国情報コミッショナー事務局（ICO）には、英国から第三国へのデータ移転に関する独自のSCCを発行する権限があるからだ。ICOのウェブサイトによると、ICOは現在、英国独自のSCCを開発中であり、パブリックコメントの募集と欧州データ保護委員会（EDPB）の意見聴取を受ける予定だ。英国SCCが最終決定されるまで、ICOは企業に対し、新規契約ではEU SCCを引き続き使用するよう勧告している。これらの条項は、英国のデータ保護法において有効な移転メカニズムとして認められているからだ。ただし、ICOは企業に対し、英国がEU加盟国ではなくなったことを反映させるためにEU SCCを修正する必要がある場合があり、英国SCCが利用可能になり次第、契約を更新する必要があるとも警告している。
参照：
GDPR、第3条、第4条、第28条、第29条、第32条、第44条、第45条、第46条、第47条、第48条、第49条。
新しい標準契約条項 - 質問と回答の概要、段落 1、2、3、4、5、6、7、8、9、10、11。
標準契約条項（SCC）の第 1 項、第 2 項、第 3 項、第 4 項、第 5 項、第 6 項、第 7 項、および第 8 項。
[国際データ転送の使用]、第1項、第2項、第3項、第4項、第5項、第6項、第7項、第8項、第9項、および第10項。

最新問題: **195**
BYOD (個人所有デバイス持ち込み) プログラムを導入している組織にとって、最も重大な課題となる GDPR 要件はどれですか?
A. データ主体は、個人データが処理される目的について十分に知らされなければなりません。
B. 特別なカテゴリの個人データを大規模に処理するには、DPO を任命する必要があります。
C. データ主体の個人データは常に正確かつ最新の状態に保たれなければなりません。
D. データ管理者は、保有するデータを常に管理する必要があります。

Answer: D (メーッセージを残す)
無料CIPP/E学習ガイドの12ページには、 GDPRは、データ管理者に対し、処理がGDPRに準拠していることを保証し、かつその証明を可能にするために、適切な技術的および組織的措置を実施することを義務付けています。これらの措置は、処理の性質、範囲、状況、目的に加え、自然人の権利と自由に対する様々な発生可能性と重大性のリスクを考慮する必要があります。」と記載されています。GDPRはまた、データ管理者に対し、個人データのセキュリティを確保し、データ侵害を監督当局とデータ主体に通知し、監督当局と協力して業務遂行に必要な情報を提供することを義務付けています。したがって、データ管理者が保有するデータを常に管理しなければならないというGDPRの要件は、BYODプログラムを実施する組織にとって最も重大な課題となります。従業員や請負業者による個人デバイスの使用によって生じる可能性のある、データの損失、盗難、不正アクセス、または悪用のリスクの増大に対処する必要があるからです。その他の選択肢は、BYODプログラムを実施している組織にとって必ずしも困難ではありませんが、有効な法的根拠の取得、適切な保護措置の提供、データ主体への情報提供など、GDPRに基づくその他の義務を伴う場合があります。参考：
無料のCIPP/E学習ガイド、12ページ
GDPR、第24条、第25条、第28条、第32条、第33条、第34条、および第58条

最新問題**: 196**
GDPR では、個人データを収集する前に、データ主体にどのような重要な情報を提供しなければならないのでしょうか?
A. コントローラーがデータを収集する権限と、データが送信される第三者。
B. 関係する政府機関の名前とデータの修正に必要な手順。
C. 管理者の ID と連絡先の詳細、およびデータが収集される理由。
D. コントローラーの連絡先情報と保持ポリシーの説明。
Answer: C (メーッセージを残す)
GDPRでは、個人データが収集される際に、データ主体自身または他の情報源から特定の情報を提供することが義務付けられています12。この情報には、管理者 および該当する場合は管理者の代理人およびデータ保護責任者）の身元情報および連絡先、個人データの処理目的、および処理の法的根拠が含まれます34。この情報は、個人データの公正かつ透明な処理を確保し、データ主体がGDPRに基づく権利を行使できるようにするために必要です5。
したがって、選択肢Cは、個人データの収集前にデータ主体に提供しなければならない必須情報のうち2つを含んでいるため、正解です。選択肢A、B、Dは、必要な情報がすべて含まれていないか、必須ではない情報が含まれているため、不正解です。参考文献 :1： 記事 GDPR第13条 2: GDPR第14条 3: GDPR第13条(1)(a)項および 4: GDPR第14条(1)(a)項および 5: GDPR第60条

最新問題**: 197**
GDPR に新しく導入されたメカニズムのうち、第 42 条に基づいて第三国への個人データの転送を可能にするものはどれですか。
A. 拘束力のある企業規則。
B. 標準契約条項。

C. 法執行機関からの要請。
D. 承認された認定資格。
Answer: D (メーッセージを残す)

最新問題**: 198**
シナリオ
次の質問に答えるには、以下を使用してください。
ABCホテルチェーンとXYZ旅行代理店は、米国を拠点とする多国籍企業です。両社は、マーケティング活動を統合するために、インターネットベースの共通プラットフォームを使用して顧客データを収集 -共有しています。さらに、両社は、保存するデータ、予約の受付方法と確認方法、そして保存データへのアクセス権について合意しています。
EU在住のマイクは、過去にXYZ旅行代理店を通じてABCホテルチェーンの宿泊施設に宿泊する旅行プランを予約したことがあります。XYZ旅行代理店は、会員登録するとポイントが貯まり、後日無料旅行と交換できるリワードプログラムを提供しています。マイクはリワードプログラム会員契約に署名しました。
マイクは、会社が自分の個人情報をどのように保有しているかを知りたいと考え、データ主体としての権利を行使するため、データへのアクセスを要求するメールを送信しました。
マイクがリクエストに対する返答を受け取るまでの期間はどれくらいですか?
A. Mike のリクエストを受け取ってから 1 か月以内。
B. マイクの身元を確認してから 2 か月以内。
C. Mike に関するすべての情報が収集されたとき。
D. Mike のリクエストが提出されてから 30 日以内。
Answer: A (メーッセージを残す)
GDPRによれば、データ主体によるアクセス権は、データ管理者による個人データの処理に関する情報を取得するために個人に付与される権利の一つです1。データ管理者は、処理中の個人データのコピーに加え、処理の目的、カテゴリー、受信者、保存期間、権利、情報源、処理の自動化された意思決定などの追加情報を提供しなければなりません1。また、データ管理者は、データ主体に対し、アクセス権の存在とその行使手段について通知しなければなりません2。
GDPRは、データ主体からのアクセス要求への回答期限も規定しています。データ管理者は、要求の受領後1ヶ月以内に、遅滞なく情報を提供しなければなりません1。この期間は、要求の複雑さや件数を考慮し、必要に応じてさらに2ヶ月延長することができますが、データ管理者は、要求の受領後1ヶ月以内に、データ主体に対し、そのような延長について、遅延の理由とともに通知しなければなりません1。また、データ管理者は、情報提供前にデータ主体の身元を確認する必要がありますが、この確認によって要求への回答期限が延長されることはありません3。
このシナリオでは、マイクはEU在住者で、XYZ旅行代理店を通じて旅行プランを予約し、ABCホテルチェーンの施設に宿泊しました。両社は米国に拠点を置く多国籍企業であり、顧客データの収集と共有に共通のプラットフォームを使用しています。マイクはXYZ旅行代理店のリワードプログラム会員契約に署名しました。マイクは同社が保有する個人情報について知りたいと考え、データへのアクセスを要求するメールを送信しました。
両社がEU域内の個人に商品やサービスを提供しているため、あるいはEU域内の個人の行動を監視しているためにGDPRの対象となると仮定すると、両社はデータ主体のアクセス権を遵守し、マイク氏に要求された情報を提供しなければなりません。マイク氏が要求への回答を受け取るべき期間は、期間を2か月延長する根拠がない限り、要求受領後1か月以内です。両社は情報提供前にマイク氏の本人確認を行う必要がありますが、この確認は要求への回答期限に影響を与えてはなりません。
したがって、正解は A です。マイクのリクエストを受け取ってから 1 か月以内です。

最新問題: **199**
次のどれが、GDPR の第 5 条第 2 項に規定されている説明責任の原則に準拠していることを示していますか?
A. 特別なカテゴリのデータを匿名化します。
B. データ保護プログラムの定期的な監査を実施します。
C. 国境を越えたデータ転送についてデータ主体から同意を得る。
D. 強力な暗号化アルゴリズムを使用して、転送中および保存中のデータを暗号化します。
Answer: B (メーッセージを残す)
GDPR第5条第2項に規定されている説明責任の原則は、データ管理者に対し、GDPRの遵守に責任を負い、その遵守を実証できることを求めています1。これは、データ管理者が個人データをGDPRに従って処理していることを保証し、実証するために、適切な技術的および組織的措置を実施しなければならないことを意味します2。説明責任の原則への遵守を実証できる措置の一つは、データ保護プログラムの定期的な監査の実施です。監査とは、組織のデータ処理活動、データ保護ポリシーおよび手順を体系的かつ独立的に評価することです3。監査は、データ保護プログラムにおけるギャップやリスクを特定し、対処するとともに、データ保護措置の有効性と効率性を検証するのに役立ちます3。また、監査は監督当局とデータ主体に遵守の証拠を提供し、組織の信頼と評判を高めることにもつながります3。したがって、データ保護プログラムの定期的な監査の実施は、説明責任の原則への遵守を実証する方法の一つです。参考文献 :1 :CIPP/E学習ガイド、15ページ、GDPR第5条、説明責任の原則 | ICO2: CIPP/E 学習ガイド、16 ページ; GDPR 第 24 条; [説明責任とガバナンスのガイド | ICO]3: CIPP/E 学習ガイド、91 ページ; [監査 | ICO]; [GDPR 監査: 知っておくべきこと - IT ガバナンス ブログ]。

最新問題: **200**
米国企業のウェブサイトではウィジェットを販売しています。以下の要素のうち、それ自体ではGDPRの対象とならないものはどれですか？
A. ウィジェットは EU で提供され、価格はユーロで設定されます。
B. ウェブサイトは英語とフランス語で提供されており、フランスからアクセスできます。
C. 関連オフィスはフランスにありますが、処理は米国で行われます
D. ウェブサイトは、EU ウェブサイトのユーザーの行動を監視するために Cookie を配置します。
Answer: (解答を表示する)
GDPR によれば、処理が EU 内で行われるか否かに関わらず、EU 内に管理者または処理者の拠点がある活動に関連して行われる個人データの処理に、この規則が適用されます1。GDPR は、EU 内に拠点がない管理者または処理者による、EU 内にいるデータ主体の個人データの処理にも適用され、処理活動は次に関連します。(a) データ主体の支払いが必要かどうかに関わらず、EU 内のそのようなデータ主体に商品またはサービスを提供すること、または (b) EU 内で行われる限り、その行動を監視すること1。
このシナリオでは、米国企業のウェブサイトがEUの顧客にウィジェットを販売し、顧客の行動を監視するためにCookieを配置しています。これらの要素は、企業がEU域内の商品またはサービスを提供し、データ主体の行動を監視していることを示しているため、GDPRの対象となります2。しかし、ウェブサイトが英語とフランス語で提供され、フランスからアクセス可能であるという事実自体は、必ずしもEU域内の顧客をターゲットとする意図を示唆するものではないため、GDPRの対象にはなりません3。ウェブサイトの言語とアクセシビリティは、EU域内における企業の活動の安定性と継続性について、関連性と妥当性を十分に証明するには不十分です3。したがって、正解はBです。
参照：
GDPR第3条 - 適用範囲

GDPRの適用範囲に関するガイドライン3/2018（第3条）
GDPR における地域範囲とはどういう意味ですか?
GDPRとその適用範囲についてご理解を深めていただければ幸いです。他にご質問がございましたら、お気軽にお問い合わせください。

最新問題: **201**
データ侵害が発生した場合、データ管理者が監督当局またはデータ主体に提供する必要がない情報の種類はどれですか?
A. 侵害の予測される結果。
B. 違反に対処するために講じられている対策。
C. データを保護するために使用されるセキュリティ保護手段の種類。
D. 適切なデータ保護責任者の連絡先の詳細。
Answer: A (メーッセージを残す**)**
CIPP/E 学習ガイドによると、GDPR の第 33 条では、データ管理者は、個人データの漏洩が自然人の権利と自由にリスクをもたらす可能性が低い場合を除き、過度の遅延なく、可能であれば、漏洩を認識してから 72 時間以内に監督機関に通知する必要があります。1GDPR の第 34 条では、データ管理者は、漏洩が自然人の権利と自由に高いリスクをもたらす可能性がある場合、過度の遅延なく、個人データの漏洩をデータ主体に伝える必要があります 2。両条項では、データ管理者が監督機関とデータ主体に提供する必要がある最低限の情報が規定されており、これには、漏洩の性質、関係するデータ主体と個人データ記録のカテゴリと概数、データ保護責任者またはその他の連絡先担当者の名前と連絡先、漏洩の可能性のある結果、および漏洩に対処してその悪影響を軽減するために講じられた、または提案された措置が含まれます12。しかし、どちらの条項も、データ管理者がデータ保護に用いるセキュリティ対策の種類を開示することを義務付けていない。この情報は通知の目的とは無関係であり、データのセキュリティをさらに損なう可能性もあるためである3。参考文献 :1 :CIPP/E学習ガイド、84ページ ;GDPR第33条 ;データ漏洩通知に関する事例に関するガイドライン01/20212 :CIPP/E学習ガイド、85ページ ;[GDPR第34条] ;ガイドライン01
/2021 データ侵害通知に関する例3: 個人データ侵害 | 欧州データ保護監督官; データ侵害とは何か、そして私たちは何をしなければならないのか... - 欧州委員会。
参考: https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact- assessments

最新問題: **202**
2009 年の電子プライバシー指令 2002/58/EC の改正によって導入された変更点は何ですか?
A. すべてのデータ管理者に適用される個人データ侵害に関する自主的な通知。
B. 電子通信プロバイダーに適用される個人データ侵害に関する自主的な通知。
C. すべてのデータ管理者に適用される個人データ侵害に関する必須通知。
D. 電子通信プロバイダーに適用される個人データ侵害に関する必須通知。
Answer: D (メーッセージを残す**)**
電子プライバシー指令2002/58/EC（プライバシーと電子通信に関する指令とも呼ばれる）は、GDPRを電子通信分野向けに補完し、特化した指令です。2009年には指令2009/136/ECによって改正され、電子通信分野における個人データとプライバシーの保護を強化するためのいくつかの変更が導入されました。これらの変更の一つとして、電気通信事業者やインターネットサービスプロバイダなど、公開されている電子通信サービスを提供する事業者に適用される、個人データ漏洩に関する通知義務の導入が挙げられます。

改正電子プライバシー指令第 4 条によれば、これらのプロバイダーは、コミュニティ内で公開されている電子通信サービスの提供に関連して送信、保存、またはその他の方法で処理された個人データの偶発的または違法な破壊、紛失、変更、不正開示、またはアクセスにつながるセキュリティ侵害を管轄の国家機関に通知する必要があります。
通知は、不当に遅滞することなく、可能であれば、プロバイダが侵害を認識してから24時間以内に行われなければなりません。通知には、関係する個人データの性質と内容、侵害の状況と結果、プロバイダが侵害に対処するために講じたまたは提案した措置などの情報が含まれていなければなりません。プロバイダは、アクセス権限のない者がデータを理解できないようにする適切な技術的保護措置を実施していることを管轄当局が納得できる形で証明しない限り、影響を受けたデータ主体にも侵害を通知しなければなりません。データ主体への通知には、侵害の性質と詳細情報を入手できる連絡先を記載し、侵害による潜在的な悪影響を軽減するための措置を推奨しなければなりません。この義務的な通知の目的は、当局とデータ主体に侵害に関連するリスクと救済策を確実に周知し、プロバイダがセキュリティ対策を改善し、さらなる侵害を防止するよう促すことです。参照：電子プライバシー指令、欧州議会で承認された電子プライバシー指令の改正、指令2002/58/EC（プライバシーと電子通信に関する指令）の第2条改正、個人データの侵害

最新問題: **203**
スペインの電力会社顧客が、地元の電力会社に電話をかけ、会社の合併について質問しました。具体的には、合併が成立した後、自分の個人データが誰に開示されるのかを知りたいとのことです。GDPR第13条によれば、会社は顧客に要求された情報を提供する前に何をしなければならないのでしょうか？
A. 要求が GDPR の発効前に収集されたデータに適用可能であることを確認します。
B. 顧客からのリクエストの目的が GDPR に準拠していることを確認します。
C. 個人データが顧客にまだ送信されていないことを確認します。
D. 顧客の身元が他の手段で証明できることを確認します。
Answer: A (メーッセージを残す**)**
参考 :https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf

最新問題: **204**
GDPR に基づいてデータ主体に明示的に付与される権利ではないものはどれですか?
A. 管理者が保有するデータの削除を要求する権利。
B. 管理者が保有する個人データへのアクセスを要求する権利。
C. 第三者への個人データの販売を拒否する権利。
D. 特定のシナリオ下で個人データの処理の制限を要求する権利。
Answer: B (メーッセージを残す**)**

最新問題: **205**
ある団体のウェブサイトは、EUユーザーのパソコンおよびモバイルデバイスのブラウザにテキストファイルを保存します。その前に、当該団体は、以下のどの枠組みに基づいて、情報と同意を含む通知をユーザーに提供する必要がありますか？
A. 一般データ保護規則 2016/679。
B. 電子プライバシー指令 2002/58/EC。
C. 電子商取引指令 2000/31/EC。
D. データ保護指令 95/46/EC。
Answer: B (メーッセージを残す**)**

こんにちは、Bingです。ご質問の解決に向けて、ウェブ上の関連情報をご提供することは可能ですが、情報の正確性や完全性を保証することはできず、回答の検証もできません。CIPP/E認定試験については、必ず公式の情報源や資料をご確認ください。
ウェブ検索の結果から判断すると、最も可能性の高い答えはB. 電子プライバシー指令2002/58/ECです。その理由を以下にまとめます。
* 電子プライバシー指令2002/58/EC1は、データ保護指令95/46に定められた一般的なデータ保護原則を補完し、特定化する特定の法的枠組みです。
/EC1（一般データ保護規則 2016/6792 に置き換えられました）。
* 電子プライバシー指令 2002/58/EC1 は、Cookie や類似のテクノロジーの使用を含む、電子通信分野における個人データの処理とプライバシーの保護を対象としています3。
* 電子プライバシー指令 2002/58/EC1 の第 5.3 条では、加入者またはユーザーの端末機器に情報を保存したり、すでに保存されている情報にアクセスしたりすることは、当該加入者またはユーザーが明確かつ包括的な情報を提供されて同意した場合にのみ許可されると規定されています14。
* したがって、EU ユーザーのコンピューターやモバイル デバイスのブラウザーにテキスト ファイル (Cookie など) を保存する組織の Web サイトは、電子プライバシー指令 2002/58/EC1 に準拠し、その前に情報と同意を含む通知をユーザーに提供する必要があります45。

最新問題**: 206**
シナリオ
次の質問に答えるには、以下を使用してください。
ジョーは2000年に米国バーモント州の自宅でグミベアカンパニーを設立しました。
現在、同社は数十億ドル規模のキャンディー会社として、全大陸で事業を展開しています。同社のITサーバーはすべてバーモント州に設置されています。今年、ジョーは息子のベンを会社に迎え入れ、わずか5年で総売上高を3倍にするという大規模なマーケティング戦略「プロジェクト・ビッグ」の責任者に任命しました。ベンは一流大学でコンピュータソフトウェアの博士号を取得しています。ベンは父親の会社に加わることを決めましたが、同時に「ベン・ノウズ・ベスト」という新しいグローバルオンラインデートサイト会社の立ち上げにも密かに取り組んでいます。
ベンは、グミベア・カンパニーが何百万人もの顧客を抱えていることを認識しており、その多くが理想のパートナーを見つけることに興味を持っているかもしれないと考えています。プロジェクト・ビッグでは、ベンは同社のオンライン・ウェブポータルを再設計し、EUおよびその他の地域の顧客に、顧客維持のために追加の個人情報の提供を求めます。プロジェクト・ベンは、顧客の哲学的信条、政治的意見、婚姻状況に関するデータの収集を開始します。
顧客が独身の場合、ベンはその顧客の個人データをすべてベン・ノウズ・ベストの別のデータベースにコピーします。ベンは、顧客一人ひとりに情報提供前にチェックボックスにチェックを入れるよう明確に同意を求めているため、何も悪いことはしていないと考えています。プロジェクト・ビッグは重要なプロジェクトであるため、ベンの支援のため、コンピューターサイエンスを専攻する大学1年生のサムも採用しています。
ベンが声をかけると、サムはベン・ノウズ・ベストのデータベースを見つける。サムは10人の友人とスプリング・ビーク号でアイルランドへ行く予定なので、アイルランド在住の顧客情報をすべてコピーして、アイルランド滞在中に友人と連絡が取れるようにする。
ジョーは、親友の娘でアメリカのロースクールを卒業したばかりのアリスを、会社の新しい法務顧問として採用しました。アリスはGDPRについて聞いていたので、調べてみました。そしてジョーに近づき、EU域内の事業所から米国への社内データ転送のための法的メカニズムを整備することが会社にとって重要であるため、会社全員が遵守すべき拘束的企業準則（BCR）を起草したと伝えました。

ジョーはアリスの素晴らしい仕事ぶりを高く評価し、米国連邦裁判所で会社に対して提起された大規模な訴訟の処理もアリスに任せると伝えた。訴訟に備えるため、アリスは会社のIT部門に指示し、EUを含む全世界の営業チームのコンピューターのハードドライブのコピーを作成し、全てをアリスに送ってもらい、全員の情報を確認できるようにする。アリスは、自分が第一段階のレビューを担当してくれたことで、ジョーはきっと喜ぶだろうと確信している。なぜなら、これにより、本来であれば外部の法律事務所に支払うはずだった多額の費用を節約できるからだ。
ベンが会社に顧客から追加のデータを収集させたとき、データの処理によって何が作成されたため、GDPR の最も重大な違反が発生しましたか?
A. インフォームドコンセントのメカニズムが欠如しているため、重大なリスクがあります。
B. 顧客からの潜在的な法的責任および財務上のリスク。
C. データを新しいデータベースにコピーすることによる情報セキュリティ上のリスク。
D. 顧客の基本的権利と自由に対する重大なリスク。
Answer: D (メーッセージを残す)

最新問題: **207**
シナリオ
次の質問に答えるには、以下を使用してください。
ABCホテルチェーンとXYZ旅行代理店は、米国を拠点とする多国籍企業です。両社は、マーケティング活動を統合するために、インターネットベースの共通プラットフォームを使用して顧客データを収集 -共有しています。さらに、両社は、保存するデータ、予約の受付方法と確認方法、そして保存データへのアクセス権について合意しています。
EU在住のマイクは、過去にXYZ旅行代理店を通じてABCホテルチェーンの宿泊施設に宿泊する旅行プランを予約したことがあります。XYZ旅行代理店は、会員登録するとポイントが貯まり、後日無料旅行と交換できるリワードプログラムを提供しています。マイクはリワードプログラム会員契約に署名しました。
マイクは、会社が自分の個人情報をどのように保有しているかを知りたいと考え、データ主体としての権利を行使するため、データへのアクセスを要求するメールを送信しました。
この関係において、ABC ホテルチェーンと XYZ 旅行代理店の役割は何ですか?
A. XYZ 旅行代理店が管理者であり、ABC ホテルチェーンが処理者です。
B. ABC ホテルチェーンが管理者であり、XYZ 旅行代理店が処理者です。
C. ABC ホテルチェーンと XYZ 旅行代理店は独立した管理者です。
D. ABC ホテルチェーンと XYZ 旅行代理店は共同管理者です。
Answer: D (メーッセージを残す)

最新問題: **208**
GDPR では 処理」をどのように定義していますか?
A. データが収集された目的に適合する個人データの使用または開示。
B. 個人データの収集および記録を伴う行為。
C. 個人データまたは個人データ セットに対して自動化された手段によって実行される操作または操作のセット。
D. 個人データまたは個人データ セットに対して実行される任意の操作または操作のセット。
Answer: (解答を表示する)

最新問題: **209**
シナリオ
次の質問に答えるには、以下を使用してください。
Dynaroux Fashion（以下Dynaroux」）は、アイルランドのダブリンに本社を置き、約650名の従業員を擁する、国際的なオンライン衣料品小売業者です。ロナンは最近、同社のデータ保護責任者に任命され、一般データ保護規則（GDPR）およびその他のプライバシー法の遵守を監督しています。
同社は、子供を含むあらゆる年齢層を対象に、男性用と女性用の衣料品ラインを提供しています。その過程で、顧客の嗜好やクレジットカード番号や銀行口座番号といった機密性の高い金融情報など、大量の顧客情報を処理しています。
収益成長を積極的に図るため、CEOのジョナスはロナンに対し、顧客の購入履歴を分析することで顧客のプロファイリングに重点を置いた新しいモバイルアプリとロイヤルティプログラムを導入することを伝えた。ロナンはCEOに対し、(a) こうした活動には潜在的なリスクがあるため、ダイナルーはデータ保護影響評価を実施し、この新しい取り組みとプライバシーへの影響を評価する必要があること、(b) この評価結果が、適切な保護措置を講じない場合に高いリスクをもたらすことを示している場合、ダイナルーはアプリとロイヤルティプログラムを導入する前に、アイルランドのデータ保護コミッショナーと事前協議を行う必要がある可能性があることを伝えた。
ジョナス氏はロナン氏に対し、監督当局と直接交渉し、ディナルー社の事業計画や関連する処理活動の詳細を開示しなければならない可能性について不満を述べている。
Dynaroux に関する次の事実のうち、GDPR に基づくデータ保護影響評価のきっかけとなるものはどれですか?
A. 当社は、財務データや児童データなどの機密データカテゴリに関連する処理活動を実施します。
B. 当社は約 650 人の従業員を雇用しており、広範な処理活動を行う予定です。
C. 同社は顧客の購買パターンを分析し、顧客のプロファイリングを行う予定です。
D. 同社は、ビジネスモデルを転換し、オンラインショッピングに重点を置く予定です。
Answer: C (メーッセージを残す)
無料CIPP/E学習ガイドの14ページによると、「GDPRは、特に新しい技術を用いた処理、ならびに処理の性質、範囲、状況および目的を考慮した上で、自然人の権利および自由に高いリスクをもたらす可能性のある処理の種類について、管理者に対し、処理前にデータ保護影響評価（DPIA）を実施することを義務付けています。」GDPRはまた、DPIAが必要となる処理業務の例として、「プロファイリングを含む自動化された処理に基づき、自然人に関する個人的側面の体系的かつ広範な評価を行い、その評価に基づいて、自然人に関する法的効果を生じさせる、または同様に自然人に重大な影響を与える決定を行うもの」（第35条(3)(a)）を挙げています。したがって、Dynarouxが顧客の購買パターン分析を通じて顧客のプロファイリングを行う計画は、顧客に重大な影響を与える可能性のある自動化された処理に基づく個人的側面の体系的かつ広範な評価を伴うため、GDPRに基づくDPIAの対象となると考えられます。その他の選択肢は、有効な法的根拠の取得、適切な保護措置の提供、データ主体への通知など、GDPRに基づくその他の義務を伴う場合がありますが、必ずしもDPIAが必要となるケースではありません。参考資料：
* 無料のCIPP/E学習ガイド、14ページ
* GDPR第35条

最新問題: **210**
EU 法に基づく権利の行使を希望する個人の行動について決定を下すのはどの司法機関ですか?
A. 会計検査院
B. 欧州連合司法裁判所
C. 欧州人権裁判所

D. 欧州データ保護委員会
Answer: B (メーッセージを残す**)**
欧州連合司法裁判所（CJEU）は、EU法に関する問題について判決を下し、欧州委員会が加盟国に対して行った措置、または個人がEU法に基づく権利を行使するために行った措置に関して、EUの決定を執行するEUの司法機関です。CJEUは、司法裁判所と一般裁判所の2つの裁判所で構成されています。CJEUは、EU法のEU全体にわたる統一的な解釈と適用を確保し、EU機関、加盟国、および個人間の紛争を解決します。
その他の選択肢は正しくありません。なぜなら、それらはEU法に基づく権利の行使を希望する個人の行動について決定を下す司法機関ではないからです。会計検査院はEUの独立した外部監査機関であり、EUの歳入と歳出の合法性と規則性、そして財政運営の健全性を検査します。欧州人権裁判所（ECHR）は、1950年の欧州人権条約を監督する国際裁判所です。ECHRはEU機関とは連携しておらず、多くの非EU諸国を含むヨーロッパ全域の人権法を管轄しています。欧州データ保護委員会（EDPB）は、GDPRの一貫した適用を確保し、データ保護のさまざまな側面について意見を表明する独立機関ですが、司法権は持ちません。
参考文献:
欧州連合司法裁判所
欧州連合司法裁判所 - 国際プライバシー専門家協会 EU法の司法執行 | 生活・労働条件改善のための欧州財団 欧州連合司法裁判所の権限

最新問題**: 211**
GDPR第13条および第14条は、個人データを収集する際にデータ管理者がデータ主体に通知する義務について詳細に規定しています。ただし、両条とも、データ主体が既に情報を保有している場合については例外を規定しています。
他にどのような状況でデータ管理者が第 14 条に基づくこの義務から免除されるでしょうか?
A. 情報を提供することが警察の命令に反する場合。
B. 情報提供に過度の労力がかかる場合
C. 個人データがパブリックドメインの複数のソースから取得された場合
D. GDPR発効の5年前に個人データが取得された場合
Answer: B (メーッセージを残す**)**
GDPR 第 14 条によれば、データ管理者は、データ主体以外の情報源から個人データを収集する際に、データ主体に特定の情報を提供しなければなりません1。ただし、この義務には、データ主体がすでに情報を保有している場合、またはそのような情報の提供が不可能または過度の労力を伴う場合など、いくつかの例外があります2。後者の例外は、たとえば、個人データが多数の情報源から収集される場合、または個人データが公共の利益のためのアーカイブ目的、科学的または歴史的研究目的、または統計目的で処理される場合に適用される場合があります3。データ管理者は、データ主体の権利と利益を保護するために適切な措置を講じ、情報を公開する必要があります2。参照: 1: GDPR 第 14 条 - データ主体から個人データを取得していない場合に提供される情報2: GDPR 第 14 条 (5) (b)3: GDPR 説明文 62

最新問題: **212**
GDPRおよび欧州司法裁判所のSchrems II判決に準拠するため、欧州委員会は、一般的に新しい標準契約条項 (SCC)と呼ばれるものを発行しました。その結果、企業は以下のすべてを実施する必要がありますが、次の項目は除きます。
A. SCC に新しい当事者を追加することを明示的に許可する、新しいオプションのドッキング条項を検討してください。
B. 2021 年 9 月 27 日より前に締結され、古い SCC を使用しているすべての契約を、2022 年 12 月 27 日までに新しい SCC に移行します。
C. 企業がデータ輸入者である場合は、2021 年 9 月 27 日時点で新しい SCC を使用して、新しい SCC をサプライ チェーンの関連部分に伝達するための手順を実行します。
D. 英国情報コミッショナー事務局には独自の SCC セットを公開する権限がないため、Brexit 後に英国で新しい SCC を実装します。
Answer: D (メーッセージを残す**)**
一般データ保護規則 (GDPR)は、承認された認証に基づき、適切なデータ保護水準を確保していない第三国または国際機関への個人データ移転のためのメカニズムを導入しています。GDPR第46条によれば、適切なデータ保護措置を保証する契約条項は、EUから第三国へのデータ移転の根拠として使用することができます。これには、欧州委員会によって 事前承認」されたモデル契約条項、いわゆる標準契約条項 (SCC)が含まれます。
2021年6月4日、欧州委員会は、EU/EEA域内 (またはGDPRの適用対象となる)の管理者または処理者からEU/EEA域外 (GDPRの適用対象外)に設立された管理者または処理者へのデータ移転について、GDPRに基づく最新の標準契約条項 (SCC)を発行しました。これらの最新のSCCは、以前のデータ保護指令95/46に基づいて採択された3セットのSCCに代わるものです。欧州委員会は、SCCの活用に関する実用的なガイダンスを提供し、GDPRに基づくコンプライアンスへの取り組みにおいて関係者を支援するため、質疑応答(Q&A)を作成しました。
Q&A では、企業は以下のすべてを実行する必要があると述べられています。
SCC に新しい当事者を追加することを明示的に許可する、新しいオプションのドッキング条項を検討してください。
Q&Aによると、ドッキング条項は、当初の契約に含まれていなかった管理者および処理者が、後日、データの輸出者または輸入者としてSCCに加入することを可能にするものです。この条項は、複雑な処理チェーンにおけるSCCの利用を容易にし、複数の契約を締結する必要性を回避させることを目的としています。
2021 年 9 月 27 日より前に締結され、古い SCC を使用しているすべての契約を、2022 年 12 月 27 日までに新しい SCC に移行してください。Q&A によると、古い SCC は 2021 年 9 月 27 日に廃止される予定です。
ただし、その日付以前に古いSCCに基づいて締結された契約は12月まで有効です。
ただし、契約の対象となる処理業務に変更はなく、これらの条項に依拠することにより、個人データの移転がGDPR第46条第1項に定める適切な保護措置の対象となることが保証されるものとします。2022年12月27日以降、旧SCCは第三国へのデータ移転の有効な法的根拠とならなくなり、代わりに新SCCを使用する必要があります。
企業がデータ輸入者である場合は、2021年9月27日以降、新しいSCCを用いて、サプライチェーンの関連部署に新しいSCCを浸透させるための措置を講じてください。Q&Aによると、新しいSCCでは、データ輸入者は、SCCに基づいて移転された個人データを処理するすべてのサブプロセッサーと契約を締結し、その契約にSCCに基づいてデータ輸入者に課せられるものと同じデータ保護義務を含めることが求められています。つまり、データ輸入者は、2021年9月27日以降、新しいSCCがサブプロセッサーに浸透していること、およびサブプロセッサーの変更があれば、異議申し立て権を持つデータ輸出者に通知する必要があることを意味します。
Q&A では、企業が以下のことを行わなければならないとは述べられていません。
英国情報コミッショナー事務局には独自のSCCを発行する権限がないため、Brexit後、英国では新しいSCCを導入する必要がある。
しかし、これは妥当な記述ではない。英国はEU離脱後も独自のデータ保護体制を有しており、英国情報コミッショナー事務局 (ICO)

には、英国から第三国へのデータ移転に関する独自のSCCを発行する権限があるからだ。ICOのウェブサイトによると、ICOは現在、英国独自のSCCを開発中であり、パブリックコメントの募集と欧州データ保護委員会（EDPB）の意見聴取を受ける予定だ。英国SCCが最終決定されるまで、ICOは企業に対し、新規契約ではEU SCCを引き続き使用するよう勧告している。これらの条項は、英国のデータ保護法において有効な移転メカニズムとして認められているからだ。ただし、ICOは企業に対し、英国がEU加盟国ではなくなったことを反映させるためにEU SCCを修正する必要がある場合があり、英国SCCが利用可能になり次第、契約を更新する必要があるとも警告している。
参考文献:
GDPR、第3条、第4条、第28条、第29条、第32条、第44条、第45条、第46条、第47条、第48条、第49条。
新しい標準契約条項 - 質問と回答の概要、段落 1、2、3、4、5、6、7、8、9、10、11。
標準契約条項（SCC）の第 1 項、第 2 項、第 3 項、第 4 項、第 5 項、第 6 項、第 7 項、および第 8 項。
[国際データ転送の使用]、第1項、第2項、第3項、第4項、第5項、第6項、第7項、第8項、第9項、および第10項。

最新問題: **213**
透明性の原則に関連して公正な処理慣行と見なされないものは次のどれですか?
A. CCTV サインに、より詳細なプライバシー通知にリンクする QR コードを提供します。
B. ハードコピーの申請書に、組織のホームページへのハイパーリンクを提供します。
C. 現場からのオンライン アプリケーションで、ジャストインタイムのコンテキスト ポップアップ プライバシー通知を提供します。
D. ウェブサイト環境で多層的なプライバシー通知を提供します。
Answer: (解答を表示する)

最新問題: **214**
シナリオ
次の質問に答えるには、以下を使用してください。
あなたは香港に拠点を置く玩具メーカーに採用されました。同社は幅広い種類の人形、アクションフィギュア、ぬいぐるみを販売しており、世界中の様々な小売店で販売されています。同社は香港以外にオフィスを構えておらず、実際には香港以外で従業員を雇用していませんが、複数の現地販売契約を締結しています。同社が製造する玩具は、ヨーロッパ、アメリカ、アジアのあらゆる有名玩具店で販売されています。同社の収益の大部分は海外販売によるものです。
同社は現在、子供たちと会話したり交流したりできるコネクテッドトイの新シリーズを発売したいと考えています。同社のCEOは、これらのおもちゃがもたらす可能性の拡大を理由に、次なる大ヒット作になると宣伝しています。人形は、数学の計算や天気など、様々なテーマについて子供たちの質問に答えることができます。各人形にはマイクとスピーカーが搭載されており、Bluetooth経由でスマートフォンやタブレットに接続できます。半径10メートル以内にあるあらゆるモバイルデバイスも、Bluetooth経由でおもちゃに接続できます。また、人形は（同じメーカーの）他の人形と連携して相互に作用し、より充実した遊び体験を提供します。
お子様がおもちゃに質問をすると、そのリクエストはクラウドに送信され、分析されます。クラウドサーバー上で回答が生成され、人形に返されます。回答は人形に内蔵されたスピーカーから聞こえるため、まるでおもちゃが実際にお子様の質問に答えているかのように聞こえます。おもちゃのパッケージには、この機能の仕組みに関する技術的な詳細は記載されておらず、インターネット接続が必要であることも記載されていません。この機能に必要なデータ処理は、南アフリカにあるデータセンターに委託されています。しかしながら、貴社は消費者向けのプライバシーポリシーを改訂し、この点について明示していません。
同社は同時に、ゲームプレイ中に獲得したキャラクターを操作できる新たなゲームシステムの導入も計画している。このシステムには、近距離無線通信（NFC）リーダーを搭載したポータルが同梱される。このデバイスがアクションフィギュアのRFIDタグを読み取

り、画面上でフィギュアが動き出す。各キャラクターにはそれぞれ固有の特徴や能力があり、ゲーム目標を達成することで追加の能力を獲得することもできる。タグに保存される情報は、フィギュアの能力に関する情報のみ。ゲーム中にキャラクターを簡単に切り替えることができ、フィギュアを家の外に持ち出してもキャラクターの能力はそのまま維持される。
この会社が GDPR に準拠する義務があるのはなぜですか?
A. 当社は EU にオフィスを構えています。
B. 当社は EU 内で従業員を雇用しています。
C. 会社のデータセンターは EU 域外の国にあります。
D. 同社の製品は EU の顧客に直接販売されています。
Answer: (解答を表示する**)**
あなたは香港に拠点を置く玩具メーカーに採用されました。同社は幅広い種類の人形、アクションフィギュア、ぬいぐるみを販売しており、世界中の様々な小売店で販売されています。同社は香港以外にオフィスを構えておらず、実際には香港以外で従業員を雇用していませんが、複数の現地販売契約を締結しています。同社が製造する玩具は、ヨーロッパ、アメリカ、アジアのあらゆる有名玩具店で販売されています。同社の収益の大部分は海外販売によるものです。
同社は現在、子供たちと会話したり交流したりできるコネクテッドトイの新シリーズを発売したいと考えています。同社のCEOは、これらのおもちゃがもたらす可能性の拡大を理由に、次なる大ヒット作になると宣伝しています。人形は、数学の計算や天気など、様々なテーマについて子供たちの質問に答えることができます。各人形にはマイクとスピーカーが搭載されており、Bluetooth経由でスマートフォンやタブレットに接続できます。半径10メートル以内にあるあらゆるモバイルデバイスも、Bluetooth経由でおもちゃに接続できます。また、人形は（同じメーカーの）他の人形と連携して相互に作用し、より充実した遊び体験を提供します。
お子様がおもちゃに質問をすると、そのリクエストはクラウドに送信され、分析されます。クラウドサーバー上で回答が生成され、人形に返されます。回答は人形に内蔵されたスピーカーから聞こえるため、まるでおもちゃが実際にお子様の質問に答えているかのように聞こえます。おもちゃのパッケージには、この機能の仕組みに関する技術的な詳細は記載されておらず、インターネット接続が必要であることも記載されていません。この機能に必要なデータ処理は、南アフリカにあるデータセンターに委託されています。しかしながら、貴社は消費者向けのプライバシーポリシーを改訂し、この点について明示していません。
同社は同時に、ゲームプレイ中に獲得したキャラクターを操作できる新たなゲームシステムの導入を計画している。このシステムには、近距離無線通信（NFC）リーダーを搭載したポータルが同梱される。このデバイスがアクションフィギュアのRFIDタグを読み取り、画面上でフィギュアが動き出す。各キャラクターにはそれぞれ固有の特徴や能力があり、ゲーム目標を達成することで追加の能力を獲得することもできる。タグに保存される情報は、フィギュアの能力に関する情報のみ。ゲーム中にキャラクターを簡単に切り替えることができ、フィギュアを自宅以外の場所に持ち出しても、キャラクターの能力はそのまま維持される。
この会社が GDPR に準拠する義務があるのはなぜですか?
A) 同社は EU 内にオフィスを構えている。B) 同社は EU 内で従業員を雇用している。C) 同社のデータセンターは EU 域外の国にある。D) 同社の製品は EU の顧客に直接販売されている。
答え
検証済みの回答: D. 同社の製品は EU の顧客に直接販売されています。
包括的説明: GDPR1の第6条(1)によれば、個人データは、商品やサービスを提供し、またはその他の方法で活動を行う組織によって処理され、それに関連して個人データの処理が正当な利益に関連すると見なされる場合があります。ここで言及されている正当な利益とは、その名前で、またはその代理で、または自身の目的で実行されるタスクの遂行から生じる利益です。ここで言及されている正当な利益とは、その名前で、またはその代理で、または自身の目的で実行されるタスクの遂行から生じる利益です。ここで言及されている正当な利益とは、その名前で、またはその代理で、または自身の目的で実行されるタスクの遂行から生じる利益です。ここで言及されている正当な利益とは、その名前で、またはその代理で、または自身の目的で実行されるタスクの遂行から生じる利益で

す。ここで言及されている正当な利益とは、その名前で、またはその代理で、または自身の目的で実行されるタスクの遂行から生じる利益です。ここでいう正当な利益とは、本人の名義で、本人に代わって、または本人自身の目的のために遂行される業務の遂行から生じる利益をいう。ここでいう正当な利益とは、本人の名義で、本人に代わって、または本人自身の目的のために遂行される業務の遂行から生じる利益をいう。

最新問題: **215**
次の手順をお読みください。
* どの従業員がどのデバイスやアプリからクラウドサービスにアクセスしているかを把握し、それらのアプリやデバイスのデータをロックダウンします。
* アプリとデバイスのコンプライアンスを監視および分析する
* アプリケーションのライフサイクルを管理する
* データ共有を監視する
組織は次のどれを実行するためにこれらの手順を実行する必要がありますか?
A. クラウドベンダーが社内データ使用ポリシーに準拠していることを確認します。
B. 安全な Bring Your Own Device (BYOD) プログラムを維持します。
C. GDPR に準拠した Privacy by Design プロセスを追求します。
D. GDPR に準拠した従業員監視プロセスを導入します。
Answer: B (メーッセージを残す**)**

最新問題: **216**
コントローラーまたはプロセッサーとして拘束的企業準則 (BCR) を使用する国際組織の適切なコンプライアンスを最もよく表す文はどれですか。
A. 従業員は、個人データがエクスポートされるたびに、特別な契約書に署名する必要があります。
B. 作業が行われている場所に関係なく、すべての従業員は規則の全体に従う必要があります。
C. すべての従業員は、現在の業務範囲が定められている管轄区域のプライバシー規制に従わなければなりません。
D. 個人データを管理する従業員は、法的強制の対象外となるため、厳格な認証手順を完了する必要があります。
Answer: B (メーッセージを残す**)**
GDPR第47条(2)(a)項によれば、拘束的企業準則（BCR）は法的拘束力を有し、共同経済活動を行う企業グループ または企業集団）の全ての関係会社（従業員を含む）に適用され、執行されなければならない1。これは、グループ内のすべての従業員が、所在地や事業管轄区域に関わらず、BCRを遵守しなければならないことを意味します。その他の選択肢は、GDPRの要件や欧州データ保護委員会（EDPB）のBCRに関するガイダンスを反映していないため、誤りです23。参考：
GDPR第47条(2)(a)
GDPRの適用範囲に関するEDPBガイドライン3/2018
規則2016/679に基づく第49条の例外に関するEDPBガイドライン2/2018

最新問題: **217**
データ保護の分野における最初の法的拘束力のある国際文書は次のどれですか?
A. 条約 108。
B. 一般データ保護規則。
C. 世界人権宣言。

D. プライバシーと電子通信に関する EU 指令。
Answer: A (メーッセージを残す**)**
参考 :https://www.coe.int/en/web/data-protection/convention108/background 個人データの自動処理に関する個人の保護に関する条約としても知られる条約108は、1981年に欧州評議会によって採択されました。これは、データ保護に関する最初の法的拘束力のある国際文書であり、署名国は、個人データの処理に関してすべての個人の基本的人権が自国で尊重されることを確保するために、国内法においてこの条約に定められた原則を適用する措置を講じることを義務付けられました1。この条約は、公共部門と民間部門の両方を対象とし、自動化の有無にかかわらず、あらゆる種類のデータ処理に適用されます。また、独立した監督機関の設立と国境を越えたデータフローの促進についても規定しています2。
その他のオプションは、次の理由により正しくありません。
B) 一般データ保護規則（GDPR）は、2018年に施行された欧州連合（EU）の規則です。これは、データ保護に関する最初の法的拘束力のある国際文書ではありませんが、1995年に採択され、EU加盟国が国内法で実施しているEU指令95/46/ECの後継です。
C) 世界人権宣言（UDHR）は、1948年に採択された国連総会決議です。法的拘束力のある国際文書ではありませんが、人権法の発展を導く共通の原則と価値観の宣言です。UDHRはデータ保護について明示的に言及していませんが、第124条においてプライバシー権を基本的人権として認めています。
D) EUプライバシー及び電子通信に関する指令（eプライバシー指令）は、2002年に採択され、2009年に改正された欧州連合の指令です。これは、データ保護に関する最初の法的拘束力のある国際文書ではありませんが、電子通信サービスにおける個人データの保護に関する追加ルールを規定することにより、EU指令95/46/ECとGDPRを補完する特定の文書です5。
参照: 5 2002年7月12日の欧州議会及び理事会の指令2002/58/EC（電子通信分野における個人データの処理及びプライバシーの保護に関する指令）| EUR-Lex53 2016年4月27日の欧州議会及び理事会の規則（EU）2016/679（個人データの処理及びそのデータの自由な移動に関する自然人の保護並びに指令95/46/ECの廃止に関する規則）| EUR-Lex34 世界人権宣言 | 国連42 条約108及び議定書 - データ保護 - 欧州評議会21 条約とは
108? - プライバシー熟練者1。

最新問題**: 218**
Planet 49 事件において、クッキーの問題に関する欧州連合司法裁判所 (CJEU) の主な判決は何でしたか?
A. クッキーが個人データを追跡しない場合は、事前にチェックされたボックスが許容されます。
B. ePrivacy 指令で Cookie への同意が必要な場合は、GDPR の同意要件が適用されます。
C. ウェブサイトの Cookie に関する通知で、収集される情報と Cookie の有効期間が明確に示されている場合は、事前にチェックされたボックスが許容されます。
D. データ主体が Cookie バナーを読んだ後も Web サイトをスクロールし続ける場合、このアクティビティは Cookie バナーに記載されている追跡に対する有効な同意を構成します。
Answer: (解答を表示する**)**
欧州司法裁判所（CJEU）は、eプライバシー指令でクッキーの使用に求められる同意は、GDPRに定められた条件を満たす必要があると判決を下しました。つまり、同意は具体的で、十分な情報に基づいた、明確な、そして自由意志に基づくものでなければなりません。したがって、チェックボックスに事前にチェックを入れたり、スクロールすることで暗黙的に同意を得たりすることは、クッキーに関する有効な同意の形式ではありません。また、欧州司法裁判所は、eプライバシー指令は、個人データであるかどうかに関わらず、ユーザーのデバイスに保存またはアクセスされるあらゆる情報に適用されることを明確にしました。さらに、欧州司法裁判所は、クッキーに関してユーザーに提供される情報には、クッキーの有効期間と第三者がクッキーにアクセスする可能性を含める必要があると述べました。

参考文献: CIPP/E 学習ガイド、29 ページ; CIPP/E 教科書、137 ページ; Planet49 事例

最新問題: **219**
データ主体がポータビリティの権利を行使できない場合はどのような場合ですか?
A. 管理者に与えられた権限を行使してタスクを実行するために処理が必要な場合。
B. データ主体との契約に従って処理が行われる場合。
C. データ主体がコントローラーにデータを提供した日時。
D. 処理が同意に基づいている場合。
Answer: (解答を表示する**)**
データポータビリティの権利は、データ処理がデータ主体の同意またはデータ主体との契約に基づく場合にのみ適用されます12。したがって、処理が公共の利益のために行われる業務、または管理者に付与された公的な権限の行使に必要な場合、データポータビリティの権利は適用されません12。これは、データ主体がそのような場合、処理の目的または手段に直接的な影響力を持たないためです3。参考文献 :1 :GDPR第20条 2 :データポータビリティの権利 | ICO 3 :データポータビリティの権利（GDPR第20条）参考文献：
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/

最新問題: **220**
シナリオ
次の質問に答えるには、以下を使用してください。
サンディは最近、2016年に設立された広告テクノロジー企業Market4Uにプライバシーおよびデータガバナンス担当バイスプレジデントとして入社しました。データインベントリの実施という最初の取り組みを通して、サンディはMarket4Uが設立以来収集してきた1,900万人のグローバル連絡先リストを保有していることを知りました。膨大なデータ量のリスクを認識していたサンディは、2018年5月以前にMarket4Uのシステムに入力された連絡先のうち、Market4Uのコンテンツに最近アクセスした連絡先を除いて、すべて削除したいと考えていました。しかし、営業担当バイスプレジデントのダンは、すべての連絡先がMarket4Uのクライアントにとって、成功したマーケティングキャンペーンや業界動向に関する有用な情報を提供しているとサンディに伝えました。
ダンはサンディに、スポーツ ･エンターテイメント業界の顧客獲得に注力したいと伝えました。この顧客獲得を支援するため、Market4Uのマーケティングチームは、Market4Uのウェブサイトフォームに、ホワイトペーパーのダウンロード、Market4Uフォーラムへの参加用アカウント作成、イベントへの参加など、いくつかの新しいフィールドを追加することにしました。これらのフィールドには、生年月日や給与などが含まれています。
ダンが Market4U のフォームに追加したい新しいフィールドに関して、サンディはダンとマーケティング チームにどのようなフィードバックを与えるべきでしょうか?
A. すべてのフィールドをオプションにします。
B. 括弧内の情報のみを要求します (年齢層や給与範囲など)。
C. フィールドは提供されるサービスに比例していないため、削除します。
D. ホワイトペーパーの提供やイベントの登録の目的には必要ないので、フィールドを削除します。
Answer: D (メーッセージを残す**)**
サンディは、ダンとマーケティングチームにこのフィードバックを伝えるべきです。これはデータ最小化の原則を反映しており、収集される個人データは適切かつ関連性があり、処理目的に必要な範囲に限定されなければならないとされています1。ホワイトペーパーのダウンロードやイベントへの登録を希望する顧客から生年月日や給与情報を収集することは、これらの目的には不要であり、

データ保護とセキュリティにリスクをもたらす可能性があります2。さらに、このような情報は、データ主体からの明示的な同意が必要であり、特定の条件下でのみ処理できる特別なデータに該当する可能性があります2。
その他のオプションは、オプションであったり括弧で囲まれていても、必要以上のデータを収集するため、データ最小化の原則に準拠していません。参考文献：
* 無料のCIPP/E学習ガイド、23ページ、セクション3.1
* CIPP/E認証、18ページ、セクション3.1
* 2023年版CIPP/E究極学習ガイド、16ページ、セクション3.1
* 原則 - 一般データ保護規則（GDPR）第5条
* 個人データの特別なカテゴリ - 一般データ保護規則（GDPR）第9条

最新問題: **221**
シナリオ
次の質問に答えるには、以下を使用してください。
ProStorageは、オランダに本社を置く多国籍クラウドストレージプロバイダーです。CEOのルース・ブラウン氏は、成長のために2本柱の戦略を立てました。1) ProStorageの顧客ベースを世界中に拡大し、2) 効果的なチームを効率的に採用してProStorageの営業部隊を増強することです。この戦略の実行は、ルースの健康状態により、最近、労働時間が制限され、潜在顧客に会うために出張することも困難になったため、複雑になっています。ProStorageの人事部とルースの首席スタッフは現在協力して、彼女のスケジュールを管理し、彼女がすべての医療予約を確実に受けられるようにしています。後者は、ルースが前回インドを旅行した際に健康上の緊急事態に見舞われ、ニューデリーで入院して以来、特に重要になっています。ルースの家族と連絡が取れなかったため、病院はProStorageに連絡し、首席スタッフと連絡を取ることができました。首席スタッフは、人事部長のメアリーと連携していました。
ルースが ProStorage を開始したときのリクエストに応じて、医師に情報を提供しました。ジャッキーが推奨する追加の対策は、UpFinance の使用に対して十分な理由は何ですか?
A. UpFinanceは十分なデータ保護対策を実施しています
B. UpFinance は監視法のない国に拠点を置いています。
C. UpFinance は創業 7 年の実績を持つ企業です。
D. UpFinanceは規制の厳しい金融業界に属しています
Answer: (解答を表示する**)**

最新問題: **222**
GDPR では、個人データがデータ主体から直接取得されない場合、次の条件を満たす場合、管理者はデータ処理に関する情報をデータ主体に直接提供することが免除されます。
A. データ主体は、自分のデータがどのように使用されるかについてすでに情報を持っている
B. データ主体にそのような情報を提供することはあまりにも問題が多い
C. 第三者のデータは、データ主体に情報を提供することで開示される。
D. データ主体のデータの処理は適切な技術的手段によって保護されている
Answer: A (メーッセージを残す**)**
According to Article 14 of the GDPR, where personal data is not obtained directly from the data subject, the controller must provide the data subject with certain information about the processing, such as the identity of the controller, the purposes and legal basis of the processing, the categories of personal data concerned, the recipients or categories of recipients of the personal data, and the rights of the data subject12. However, there are some exceptions to this obligation, as specified in Article 14(5). One of them is

when the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation is likely to render impossible or seriously impair the achievement of the objectives of that processing12. In such cases, the controller must take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available12. Reference: CIPP/E Certification - International Association of Privacy Professionals, Free CIPP/E Study Guide - International Association of Privacy Professionals, GDPR - EUR-Lex, Right to be Informed - General Data Protection Regulation (GDPR)

最新問題: **223**
個人データを仮名化するには、データ管理者は何をする必要がありますか?
A. データとデータ主体を結び付けることができる情報を別途保持します。
B. 不正なアクセスや改ざんを防ぐためにデータを暗号化します。
C. すべての間接データ識別子を削除し、安全に破棄します。
D. データは研究目的でのみ集計された形式で使用します。
Answer: (解答を表示する**)**
仮名化とは、元のデータセット（メールアドレスや名前など）を別名や仮名、つまり個人を直接特定できない値に置き換える手法です1。これは可逆的なプロセスであり、データを匿名化しますが、必要に応じて後で再識別できます1。これは、一般データ保護規則（GDPR）でデータ保護手法の一つとして強く推奨されている、よく知られたデータ管理手法です2。個人データを仮名化するには、データ管理者は、キーやコードなど、データとデータ主体を結び付ける情報をすべて別途保持し、この情報が安全に保管され、不正アクセスや再識別を防ぐための技術的および組織的な措置が講じられていることを保証する必要があります23。その他の選択肢は、暗号化や匿名化などの他のデータ保護手法を説明しているか、GDPRにおける仮名化の定義を満たしていないため、正しくありません。参考資料: GDPRに基づく仮名化、仮名化 - Wikipedia、匿名化と仮名化 | データ保護コミッショナー

最新問題: **224**
ハードウェアの故障と人為的ミスが重なり、銀行の顧客口座取引データベースの復号鍵が紛失しました。調査の結果、これはハッキングや不正行為によるものではなく、単に不運な状況の組み合わせによるものであることが判明しました。このインシデントの性質を正確に示しているのは次のうちどれですか？
A. 損失はハッキングによるものではないため、データ侵害は発生していません。
B. データが権限のない個人に公開されていないため、データ侵害は発生していません。
C. キーの紛失によりデータにアクセスできなくなったため、データ侵害が発生しました。
D. キーの紛失によりデータの機密性または整合性が失われたため、データ侵害が発生しました。
Answer: (解答を表示する**)**
データ侵害は、個人データへの不正アクセス、開示、改ざん、または破壊につながるあらゆるインシデントとして広く定義されています。選択肢AとBは一見妥当に見えるかもしれませんが、侵害の解釈が狭くなっています。
ここで重要なのは、機密性および／または完全性の喪失です。たとえ誰かが積極的にデータを盗んだわけではないとしても、銀行はもはや情報の機密性を保証することも、安全にアクセスまたは変更できないためデータの完全性を保証することもできません。これはデータに対する制御の喪失に相当し、データ侵害に該当します。
参照：
IAPP CIPP/E教科書、第5章：データ侵害通知（特に、個人データ侵害の定義）GDPR第4条（12）- 個人データ侵害の定義

最新問題: **225**
企業が敷地内で閉回路テレビ (CCTV) を使用する予定があり、GDPR コンプライアンスを懸念している場合、次の項目を除くまずすべてを実行する必要があります。
A. 適切なデータ保護機関に通知します。
B. データ保護影響評価 (DPIA) を実行します。
C. システムを操作する人のための情報保持ポリシーを作成します。
D. 映像への不正アクセスを防ぐための安全対策が講じられていることを確認します。
Answer: A (メーッセージを残す)
GDPRでは、事業所内でのCCTVの使用は個人データの処理に該当し、データ保護の原則と義務の遵守が求められます。ただし、適切なデータ保護機関（DPA）への通知は、DPAが明示的に要求している場合、またはCCTVが事前協議を必要とする高リスクの処理を伴う場合を除き、企業がCCTVを使用する前に行うべき手順ではありません。GDPRの遵守を確実にするためには、以下の手順が必要です。
データ保護影響評価（DPIA）の実施は、公共エリアの大規模または体系的な監視など、個人の権利と自由に高いリスクをもたらす可能性のあるあらゆる種類の処理において必須です。DPIAは、CCTVの使用に伴う潜在的なプライバシーリスクを特定し、軽減し、それらに対処するために講じられた対策を文書化するプロセスです。DPIAには、処理の内容、その目的と必要性、リスクとメリット、安全対策とセキュリティ対策、そして利害関係者との協議内容を含める必要があります。DPIAは、CCTVシステムの設置またはアップグレード前に実施し、定期的に、または処理内容に大きな変更があるたびに見直す必要があります。
Creating an information retention policy for those who operate the system is a good practice to ensure that the personal data collected by CCTV is not kept longer than necessary for the purpose for which it was collected, and that it is securely deleted or anonymised when no longer needed. The retention period should be determined by the specific purpose and context of using CCTV, and take into account any legal or contractual obligations, as well as the expectations and rights of the data subjects. The retention policy should also specify who is responsible for managing and deleting the CCTV footage, and how the deletion process is verified and documented.
Ensuring that safeguards are in place to prevent unauthorized access to the footage is an essential requirement to comply with the GDPR principle of integrity and confidentiality, which states that personal data must be processed in a manner that ensures appropriate security of the data, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage. The safeguards may include technical and organisational measures, such as encryption, access control, logging, audit, training, policies and procedures, that aim to protect the CCTV footage from unauthorized or unlawful access, disclosure, alteration, or destruction, both during transmission and storage. Reference: GDPR Article 35, GDPR Article 36, GDPR Article 5, CCTV and video surveillance | ICO, 5 Step Guide to Check if Your CCTV is GDPR Compliant

最新問題: **226**
ある民間企業は、フランス、ポーランド、イギリス、そして本社所在地であるドイツに拠点を有しています。同社は世界中でサービスを提供しています。サービスの大部分はドイツで設計され、他の拠点でサポートされています。しかし、サービスの一つであるSaaS（Software as a Service）アプリケーションは、ポーランドの拠点で定義・実装され、他の拠点でもサポートされています。
SaaS サービスの主たる監督機関は何ですか?
A. ドイツの連邦レベルの監督機関。
B. ドイツの地域レベルの監督機関。
C. ポーランド共和国の監督機関。
D. 欧州連合の監督機関。

Answer: (解答を表示する**)**
GDPR では、処理活動に関連する主要な施設の所在地によって主たる監督機関が決定されます。
この場合、企業の本社はドイツにありますが、SaaSアプリケーションはポーランドの事業所によって具体的に定義および実装されています。これは、当該SaaSサービスに関連する個人データの処理目的と手段を決定する上で、ポーランドの事業所が主要な役割を担っていることを示しています。したがって、この特定の処理活動については、ポーランドの監督機関が主たる監督機関となります。
参照：
GDPR第56条 - 主たる監督当局の権限
IAPP CIPP/E 教科書、第 3 章: EU 一般データ保護規則 (特に、ワンストップ ショップ メカニズムと主導監督機関に関するセクション)

最新問題**: 227**
欧州データ保護委員会 (EDPB) は、転送ツールが欧州連合 (EU) レベルに準拠した個人データ保護レベルを効果的に提供しているかどうかの再評価をいつ推奨しますか?
A. 個人データ漏洩後。
B. 3年ごと。
C. 継続的に。
D. 毎年です。
Answer: C (メーッセージを残す**)**
参考：
https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

最新問題**: 228**
SCENARIO
Please use the following to answer the next question:
TripBliss Inc. is a travel service company which has lost substantial revenue over the last few years. Their new manager, Oliver, suspects that this is partly due to the company's outdated website. After doing some research, he meets with a sales representative from the up-and-coming IT company Techiva, hoping that they can design a new, cutting-edge website for TripBliss Inc.'s foundering business.
交渉中、Techivaの担当者は、詳細なアンケートを通じて顧客情報を収集する計画について説明しました。このアンケートは、特定の旅行先に合わせて顧客の好みをカスタマイズするために活用できます。TripBliss Inc.は、年齢、収入、民族など、目標達成に最も役立つデータカテゴリーをいくつでも選択できます。オリバーはこのアイデアに満足していましたが、アンケートでは顧客からデータ収集への明確な同意を得る必要があるため、このアプローチの成功度を測る方法も必要だと考えています。Techivaの担当者は、顧客がどのようにウェブサイトを利用しているかをより深く理解するために、新しいウェブサイトのトラフィックを分析するプログラム

も導入することを提案しました。彼は、顧客のデバイスに複数のCookieを配置する計画について説明しました。これらのCookieによって、TripBliss Inc.はIPアドレスやその他の情報を収集できます。例えば、顧客がどのサイトからアクセスしたか、TripBliss Inc.のウェブサイトで過ごした時間、どのページを訪問したかなどです。これらの情報はすべてログファイルにまとめられ、Techivaは特別なプログラムを使って分析します。TripBliss Inc.は、ウェブサイトの効果を評価するために集計統計情報を受け取ります。オリバー氏はこれらのサービスにTechivaを積極的に利用しています。
Techiva 社は、長年アカウント マネージャーを務めている Leon Santos 氏にプロジェクトの分析部分の管理を委託しました。標準的な手順として、Leon 氏には TripBliss 社の Web サイトの管理者権限が与えられ、そこから収集されたログ ファイルへのアクセスを許可できます。しかし TripBliss 社にとって残念なことに、Leon 氏がこの新しいプロジェクトを引き受けたのは、Techiva に対する不満が最高潮に達していたときでした。会社から不当な扱いを受けたと感じて復讐するため、Leon 氏は趣味でハッカーをしている友人 Fred 氏に助けを求めました。2 人は協力して、Fred 氏が Techiva のシステムにハッキングしてログ ファイルを USB スティックにコピーするという計画を思いつきました。Techiva を非難するために当初 USB スティックをマスコミとデータ保護当局に送るつもりでしたが、Leon 氏は良心の呵責を感じ、計画を再考することになります。彼は代わりに、USB スティックからすべてのデータを安全に消去し、会社のアクセス制御システムを再検討する必要があることをマネージャーに伝えることにしました。
レオンがマネージャーに通知した後、プロセッサーとしての Techiva の法的責任は何ですか?
A. TripBliss Inc. に報告する必要があります。
B. 完全なシステム監査を実施する必要があります。
C. 監督当局に報告しなければなりません。
D. ウェブサイトを利用した顧客に通知する必要があります。
Answer: (解答を表示する**)**
GDPR第33条によれば、処理者は個人データ漏洩を認識した後、遅滞なく管理者に通知しなければなりません1。レオン氏とフレッド氏がデータを他者に開示しなかったとしても、ログファイルへの不正アクセスとコピーは個人データ漏洩に該当します2。したがって、処理者であるTechivaは、管理者であるTripBliss Inc.に報告する法的責任を負います。その他の選択肢は、グッドプラクティスや契約条件となる場合がありますが、処理者にとって法的義務ではありません。参考：
無料のCIPP/E学習ガイド、32ページ、セクション4.1.2
CIPP/E認証、27ページ、セクション4.1.2
Cipp-e 学習ガイド、授業ノートと要約、38 ページ、セクション 4.1.2
新しいIAPP CIPP-E試験練習問題、質問141
処理者の責任、第2項

最新問題**: 229**
もともと第 29 条作業部会によって提唱されたプライバシー通知のうち、データ収集の特定の時点で処理情報を提供する方法のため、AI ベースのテクノロジーに一般的に推奨されるのはどのような種類のプライバシー通知ですか。
A. 階層化された通知。
B. プライバシーダッシュボードの通知
C. ぎりぎりの通知。
D. 視覚化に関する通知。
Answer: B (メーッセージを残す**)**

最新問題**: 230**

GDPR 第 9 条に基づき、データ処理が明示的に禁止されていないデータ カテゴリは次のどれですか。
A. 民族的起源を明らかにする個人データ。
B. 遺伝子データを明らかにする個人データ。
C. 財務データを明らかにする個人データ。
D. 労働組合の加入を明らかにする個人データ。
Answer: C (メーッセージを残す**)**
GDPR第9条は、特別なカテゴリーの個人データの処理を禁止しています。特別なカテゴリーとは、データ主体に関する機密情報を明らかにし、その権利と自由に大きなリスクをもたらす可能性のあるデータです。GDPRでは、以下の10種類の個人データを特別なカテゴリーとして定義しています。
* 人種または民族的起源を明らかにする個人データ
* 政治的意見を明らかにする個人データ
* 宗教的または哲学的信念を明らかにする個人データ
* 労働組合への加入を明らかにする個人データ
* 遺伝子データ
* 生体認証データ（識別目的で使用される場合）
* 健康に関するデータ
* 個人の性生活に関するデータ
* 個人の性的指向に関するデータ。
回答の選択肢のうち、選択肢Cのみがこれらのカテゴリに該当しません。これは、財務データはデータ主体に関する機密情報を明らかにするものではないと考えられるためです。ただし、財務データは、合法性、公平性、透明性、正確性、セキュリティなど、GDPRの一般原則および規則の対象となります。
参考文献:
* 特別カテゴリーデータ | ICO
* GDPR第9条 特別なカテゴリーの個人データの処理
* 特別なデータのカテゴリ - 国際プライバシー専門家協会 参照: https://www.privacy-regulation.eu/en/article-9-processing-of-special-categories-of-personal-data- GDPR.htm#:~:text=Processing%20of%20personal%20data%20revealing,concerning%20a%20natural%
20人%27s%20sex

最新問題**: 231**
企業が敷地内で閉回路テレビ (CCTV) を使用する予定があり、GDPR コンプライアンスを懸念している場合、次の項目を除くまずすべてを実行する必要があります。
A. 適切なデータ保護機関に通知します。
B. システムを操作する人のための情報保持ポリシーを作成します。
C. データ保護影響評価 (DPIA) を実行します。
D. 映像への不正アクセスを防ぐための安全対策が講じられていることを確認します。
Answer: (解答を表示する**)**

最新問題**: 232**
次のうち、データ保護責任者の任命が必要となるのはどれですか?

A. 処理は250人以上の従業員を雇用する組織によって実行されます。
B. 処理は、EU 内の個人に営利目的の商品またはサービスを提供する目的で実行されます。
C. 管理者または処理者の主な活動は、財務情報または子供に関する情報の処理業務です。
D. 管理者または処理者の主な活動は、大規模なデータ主体の体系的な監視を必要とする処理操作で構成されます。
Answer: (解答を表示する**)**
GDPR第37条によれば、データ保護責任者（DPO）の指定は、以下の3つの場合に管理者と処理者に義務付けられています1。
* 裁判所が司法権限をもって行動する場合を除き、公的機関または団体によって処理が行われる場合。
* 管理者または処理者の中核活動が、その性質、範囲、および/または目的により、大規模なデータ主体の定期的かつ体系的な監視を必要とする処理業務で構成されている場合。
* 管理者または処理者の主な活動が、第 9 条に従った特別なカテゴリのデータおよび第 10 条に規定される刑事上の有罪判決および犯罪に関連する個人データの大規模な処理である場合。
GDPRでは「定期的かつ体系的な監視」や「大規模」の定義は明確にされていませんが、第29条作業部会（現在は欧州データ保護委員会に置き換えられています）はこれらの概念に関するガイダンスを提供しています2。このガイダンスによると、「定期的かつ体系的な監視」には、行動ターゲティング広告を目的としたインターネット上のあらゆる形態の追跡およびプロファイリングだけでなく、CCTVや健康データモニタリングといったオフライン活動も含まれます。また、このガイダンスでは、処理が大規模であるかどうかを判断するための基準も示されており、対象となるデータ主体の数、処理されるデータ量またはデータ項目の範囲、処理活動の期間または永続性、処理の地理的範囲などが挙げられます。
このシナリオでは、オプション D のみが、管理者または処理者が、中核業務の一環として、データ主体の定期的かつ体系的なモニタリングを大規模に行っていることを意味するため、DPO の指定が義務付けられる 2 番目のケースに明確に該当するものです。これには、たとえば、オンライン行動広告、位置追跡、ロイヤルティ プログラム、健康データ分析などが含まれます。その他のオプションは、処理の規模が大きい、またはリスクが高いことを示す他の要因と組み合わせない限り、DPO を任命する義務を発動させるのに十分ではありません。たとえば、GDPR では組織の規模や従業員数に基づく閾値が設定されていないため、オプション A は関連がありません。また、GDPR では処理の営利目的と非営利目的を区別していないため、オプション B も決定的ではありません。
オプションCでは、財務情報や児童に関する情報の処理が大規模で、特殊なカテゴリーのデータが含まれる場合、DPOが必要となる場合がありますが、これは一般的なルールではありません。参考資料：
* 1: GDPR第37条
* 2: データ保護責任者（DPO）に関するガイドライン
* 3: 2016年4月27日の欧州議会および理事会の規則（EU）2016/679、個人データの処理に関する自然人の保護およびそのようなデータの自由な移動に関する規則、ならびに指令95/46 / ECの廃止（一般データ保護規則）
* 4: https://edpb.europa.eu/sites/edpb/files/files/file1/wp243rev01_en.pdf
* 5: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
* 6: [https://edpb.europa.eu/sites/edpb/files/files/file1/wp243rev01_en.pdf]
* 7: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679] 参考: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/

最新問題**: 233**
「不当な遅延なく」という規定が遵守されていると仮定した場合、データアクセス要求に応じる期限はどれくらいですか?
A. 受領後40日以内
B. 受領後40日以内。さらに40日まで延長可能

C. 受領後1ヶ月以内。さらに1ヶ月まで延長可能。
D. 受領後1ヶ月以内。さらに2ヶ月延長される場合があります。
Answer: C (メーッセージを残す**)**
参照 :https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

最新問題**: 234**
ノートブックやハードコピー ファイルに含まれる情報など、物理的な形で存在する個人データにはどのような状況で GDPR が適用されますか?
A. 個人データが、コンピュータによる配布やファイリングなど、何らかの方法で自動化された手段によって処理される場合のみ。
B. 個人データが画像スキャンや光学式文字認識などの特定のコンピュータ処理の対象となる場合のみ。
C. 個人データが、ファイリング システムの一部を形成するように十分に構造化された方法で処理される場合のみ。
D. 個人データが、印刷、ラベル付け、スタンプなどの特定の自動処理活動の物理的な出力として生成される場合のみ。
Answer: C (メーッセージを残す**)**

最新問題**: 235**
基本的人権としてのプライバシーの起源はどの文書にありますか?
A. 1948 年の世界人権宣言。
B. 1953 年のヨーロッパ人権条約。
C. 1980 年の OECD プライバシー保護に関するガイドライン。
D. 2000 年の欧州連合基本権の代表者。
Answer: A (メーッセージを残す**)**
世界人権宣言（UDHR）は、第二次世界大戦の残虐行為への対応として、1948年に国連総会で採択されました。これは、人権と基本的自由を世界的に初めて表明した宣言とされています。第12条は、「何人も、その私生活、家族、住居若しくは通信に対して恣意的に干渉され、又は名誉及び信用に対して攻撃を受けることはない」と規定しています。
すべての人は、このような干渉や攻撃に対して法の保護を受ける権利を有する。」この条項は、プライバシーを基本的人権として位置づける根拠となり、欧州人権条約（ECHR）、OECDプライバシー保護ガイドライン、欧州連合基本権憲章（CFREU）など、その後の多くの国際条約や地域条約に影響を与えてきました。参考文献：
* IAPP CIPP/E 学習ガイド、7ページ
* [世界人権宣言]
* [世界人権宣言第12条]

最新問題**: 236**
Planet 49 CJEU 判決はどれに適用されますか?
A. 第三者によってのみ使用される Cookie。
B. 技術的に必要であると判断される Cookie。
C. アクセスされたデータが個人データであるかどうかに関係なく、Cookie が保存されます。
D. アクセスされたデータが個人データとしてのみ考慮される Cookie。
Answer: C (メーッセージを残す**)**

参照：
Planet 49 CJEU判決は、アクセスされたデータが個人情報であるか否かに関わらず、Cookieに適用されます。欧州連合司法裁判所（以下"CJEU"）は、ドイツ連邦裁判所（以下"連邦裁判所"）からの予備的判断の要請に応じて、2019年10月1日にこの判決を下しました。この事件は、eプライバシー指令およびGDPRに基づくCookieおよび類似の技術の使用に関する同意の有効性に関するものでした。
欧州司法裁判所（CJEU）は、ユーザーの端末機器に保存される情報の保存またはアクセスについて同意を求めるeプライバシー指令第5条（3）は、個人データを構成するか否かに関わらず、個人のデバイスからインストールまたはアクセスされるあらゆる情報に適用されるとの判決を下した。裁判所は、この規定の目的は、保存またはアクセスされる情報の性質に関わらず発生する可能性のある、ユーザーの私的領域への干渉からユーザーを保護することであると論じた。したがって、同意要件は、ユーザーが明示的に要求したサービスの提供に厳密に必要なCookieおよび類似の技術を除き、すべてのCookieおよび類似の技術に適用される。
欧州司法裁判所はまた、eプライバシー指令に基づくクッキーに関する同意は、GDPRの同意基準に準拠する必要があることを明確にしました。つまり、同意は自由意志に基づき、具体的かつ十分な情報に基づいた上で、かつ明確な形で、明確な肯定的な行為によって与えられなければならないということです。裁判所は、チェックボックスに事前にチェックが入っているだけでは有効な同意とはならないと判断しました。これは、ユーザーによる積極的な行動を示唆するものではないためです。また、ユーザーには、クッキーの有効期間や第三者がクッキーにアクセスできるかどうかなど、クッキーに関する明確かつ包括的な情報が提供されなければならないと述べました。参考：
惑星49の審判 - クッキーモンスターの教訓
Planet 49の決定 :クッキーを使用する組織への影響 CURIA - 結果一覧

最新問題: **237**
GDPR の地域的適用範囲が適用されないのは次のうちどれですか?
A. リスボン条約の締約国であるすべての加盟国。
B. 欧州経済領域の加盟国すべて。
C. 欧州連合のすべての加盟国。
D. すべての加盟国がパリ協定に加盟しています。
Answer: B (メーッセージを残す**)**

最新問題: **238**
一般データ保護規則の適用範囲外となるデータの種類は何ですか?
A. 仮名
B. 匿名
C. 暗号化
D. マスク
Answer: B (メーッセージを残す**)**
一般データ保護規則（GDPR）は、欧州連合（EU）および欧州経済地域（EEA）における個人の個人データの処理に適用されるデータ保護法です。個人データとは、氏名、住所、メールアドレス、電話番号など、特定された、または特定可能な自然人に関するあらゆる情報を指します12。GDPRは、匿名化された個人データ、つまり特定の個人に紐付けられない個人データには適用されません12。匿名化は、仮名の使用、データの集約または一般化、統計的手法の適用など、データから識別情報を削除またはマスキングすることで実現できます12。

したがって、GDPR の範囲外となるデータの種類は匿名化されたデータです。
参照：
B. 匿名化された個人データとは、識別された、または識別可能な生存個人に関連するあらゆる情報です。さまざまな情報が一緒に収集され、特定の個人を識別できる場合も、個人データを構成します。匿名化、暗号化、または仮名化されているが、個人を再識別するために使用できる個人データは個人データであり、GDPR の範囲に含まれます。個人が識別できない、または識別できなくなった方法で匿名化された個人データは、個人データとは見なされなくなります。データが真に匿名化されるためには、匿名化は不可逆である必要があります。

最新問題**: 239**
ノートブックやハードコピー ファイルに含まれる情報など、物理的な形で存在する個人データにはどのような状況で GDPR が適用されますか?
A. 個人データが、印刷、ラベル付け、スタンプなどの特定の自動処理活動の物理的な出力として生成される場合のみ。
B. 個人データが画像スキャンや光学式文字認識などの特定のコンピュータ処理の対象となる場合のみ。
C. 個人データが、コンピュータによる配布やファイリングなど、何らかの方法で自動化された手段によって処理される場合のみ。
D. 個人データが、ファイリング システムの一部を形成するように十分に構造化された方法で処理される場合のみ。
Answer: D (メーッセージを残す**)**
GDPRは、物理的な形態の有無にかかわらず、すべての個人データに適用されます。GDPRでは、個人データとは、氏名、識別番号、位置情報、オンライン識別子など、特定された、または特定可能な自然人に関するあらゆる情報と定義されています1。したがって、GDPRでは、自然人に直接的または間接的に結び付けられるあらゆる情報が個人データとみなされます。
ただし、GDPR では、さまざまな種類の処理活動とその法的根拠も区別しています。
処理活動とは、個人データの収集、保管、利用、開示、削除など、個人データに対して実行される操作を指します。処理活動は自動または手動で行われます。自動処理とは、人間の介入なしに技術を用いて処理活動を実行することを意味します。手動処理とは、人間の介入を用いて処理活動を実行することを意味します。
GDPRでは、個人データを含むあらゆる処理活動は、合法性、公平性、透明性、目的の限定、データの最小化、正確性、保存期間の制限、完全性、機密性といった一定の原則と条件を遵守しなければならないと規定されています。これらの原則と条件は、自動処理活動と手動処理活動の両方に適用されます。
したがって、GDPRは、個人データが物理的に存在する場合、その個人データが何らかの形で自動化された手段によって、その権利と自由に影響を及ぼす形で処理される場合にのみ適用されます。例えば、企業が紙の文書をスキャンし、一定期間が経過した後、または収集当初の目的に不要になった後も削除せずにデータベースに電子的に保存する場合（第3条）、これは物理的に存在する個人データを含む自動化された処理行為とみなされます。
ただし、GDPRは、ファイリングシステムの一部を構成するほど十分に構造化された方法で取り扱われる物理的な形態の個人データには適用されません。例えば、企業が紙の文書をスキャンしたり電子的に保存したりすることなく、氏名と日付を記したフォルダーに入れてオフィスの棚に保管している場合（第3条）、これは物理的な形態の個人データを扱う自動処理活動とはみなされません。
参考文献:
* 物理データ - GDPR概要
* GDPRが物理的な記録に与える影響 - アクセス
* 個人データ - 2018年データ保護法

最新問題**: 240**

単一のデータ保護責任者を任命したい企業グループに対する必須要件を説明しているのは次のうちどれですか?
A. 企業グループは監督当局の承認を得る必要があります。
B. 企業グループは、同様の規模と機能を持つ組織で構成されている必要があります。
C. データ保護責任者は、データ管理者の主な事業所がある国に所在する必要があります。
D. データ保護責任者は、企業が所在する各施設から容易にアクセスできる必要があります。
Answer: D (メーッセージを残す**)**
参照 :https://www.privacy-regulation.eu/en/article-37-designation-of-the-data-protection-officer-GDPR.htm

最新問題**: 241**
GDPR第84条によれば、違反に対する罰則規定は次のように定められるものとする。
A. 地域のデータ保護監督当局。
B. 欧州データ保護委員会。
C. EU委員会。
D. 加盟国。
Answer: (解答を表示する**)**
参照: https://gdpr-text.com/read/article-84/

最新問題**: 242**
シナリオ
次の質問に答えるには、以下を使用してください。
ジョーは2000年、米国バーモント州の自宅でグミベア ･カンパニーを設立しました。現在、同社は数十億ドル規模のキャンディ会社に成長し、全大陸で事業を展開しています。同社のITサーバーはすべてバーモント州に設置されています。今年、ジョーは息子のベンを会社に迎え入れ、わずか5年で総売上高を3倍にするという大規模なマーケティング戦略 「プロジェクト ･ビッグ」の責任者に任命しました。ベンは一流大学でコンピュータソフトウェアの博士号を取得しています。ベンは父親の会社に加わることを決めましたが、同時に 「ベン ･ノウズ ･ベスト」という新しいグローバルオンラインデートサイト会社の立ち上げにも密かに取り組んでいます。
ベンは、グミベア ･カンパニーが何百万人もの顧客を抱えていることを認識しており、その多くが理想のパートナーを見つけることに興味を持っているかもしれないと考えています。プロジェクト ･ビッグでは、ベンは同社のオンライン ･ウェブポータルを再設計し、EUおよびその他の地域の顧客に、顧客維持のために追加の個人情報の提供を求めます。プロジェクト ･ベンは、顧客の哲学的信条、政治的意見、婚姻状況に関するデータの収集を開始します。
顧客が独身の場合、ベンはその顧客の個人データをすべてベン ･ノウズ ･ベストの別のデータベースにコピーします。ベンは、顧客一人ひとりに情報提供前にチェックボックスにチェックを入れるよう明確に同意を求めているため、何も悪いことはしていないと考

えています。プロジェクト・ビッグは重要なプロジェクトであるため、ベンの支援のため、コンピューターサイエンスを専攻する大学1年生のサムも採用しています。
ベンが声をかけると、サムはベン・ノウズ・ベストのデータベースを見つける。サムは10人の友人とスプリング・ビーク号でアイルランドへ行く予定なので、アイルランド在住の顧客情報をすべてコピーして、アイルランド滞在中に友人と連絡が取れるようにする。
ジョーは、親友の娘でアメリカのロースクールを卒業したばかりのアリスを、会社の新しい法務顧問として採用しました。アリスはGDPRについて聞いていたので、調べてみました。そしてジョーに近づき、EU域内の事業所から米国への社内データ転送のための法的メカニズムを整備することが会社にとって重要であるため、会社全員が遵守すべき拘束的企業準則（BCR）を起草したと伝えました。
ジョーはアリスの素晴らしい仕事ぶりを高く評価し、米国連邦裁判所で会社に対して提起された大規模な訴訟の処理もアリスに任せると伝えた。訴訟に備えるため、アリスは会社のIT部門に指示し、EUを含む全世界の営業チームのコンピューターのハードドライブのコピーを作成し、全てをアリスに送ってもらい、全員の情報を確認できるようにする。アリスは、自分が第一段階のレビューを担当してくれたことで、ジョーはきっと喜ぶだろうと確信している。なぜなら、これにより、本来であれば外部の法律事務所に支払うはずだった多額の費用を節約できるからだ。
ベンが顧客から追加データを収集したことで、会社にいくつかの潜在的な問題が発生しましたが、おそらく何が必要になるでしょうか?
A. データ保護責任者の雇用。
B. 包括的なデータ インベントリ。
C. データ保護影響評価。
D. 新しい企業統治と行動規範。
Answer: (解答を表示する**)**

最新問題: 243
A company is hesitating between Binding Corporate Rules and Standard Contractual Clauses as a global data transfer solution.
Which of the following statements would help the company make an effective decision?
A. Binding Corporate Rules are especially recommended for small and medium companies.
B. The data exporter does not need to be located in the EU for the standard Contractual Clauses.
C. Binding Corporate Rules provide a global solution for all the entities of a company that are bound by the intra-group agreement.
D. The company will need the prior authorization of all EU data protection authorities for concluding Standard Contractual Clauses.
Answer: C (メーッセージを残す**)**
According to the GDPR, transfers of personal data to third countries or international organisations are only allowed if the controller or processor complies with the conditions laid down in Chapter V of the GDPR1. One of these conditions is the existence of an adequacy decision by the European Commission, which means that the third country or international organisation ensures an adequate level of protection for the personal data2. However, if there is no adequacy decision, the controller or processor must provide appropriate safeguards for the data transfer, such as binding corporate rules (BCR) or standard contractual clauses (SCC)3. Binding corporate rules (BCR) are internal rules adopted by a group of undertakings or enterprises engaged in a joint economic activity, which define its global policy with regard to the international transfers of personal data within the same corporate group or business partners located in third countries4. BCR must include all the general data protection principles and enforceable rights to ensure appropriate safeguards for the data transfers. They must be legally binding and enforced by every member concerned of the group5. BCR must be approved by the competent supervisory authority in accordance with the consistency mechanism provided by the GDPR6.

Standard contractual clauses (SCC) are sets of contractual terms and conditions that the controller or processor and the recipient of the data agree to apply to the data transfer. SCC are adopted by the European Commission or by a supervisory authority in accordance with the consistency mechanism and are available in the Official Journal of the European Union7. SCC must offer sufficient safeguards on data protection for the data to be transferred internationally8.
上記のシナリオでは、オプション C は、企業が BCR と SCC の間で効果的な決定を下すのに役立つ記述です。これは、SCC に対する BCR の主な利点、つまりグループ内契約に拘束される企業内のすべてのエンティティに BCR が提供するグローバルで包括的なソリューションを強調しているためです。BCR は、同じ企業グループ内または第三国に所在するビジネス パートナー内で頻繁かつ大量のデータ転送を行う大規模で複雑な組織に特に適しています。また、BCR はグループの特定のニーズと構造に合わせて調整され、データ転送ごとに個別の契約を必要としないため、SCC よりも柔軟性と法的確実性が高くなっています。
その他の選択肢（A、B、D）は、誤りまたは誤解を招く記述であり、企業がBCRとSCCの間で効果的な判断を下す上で役立ちません。選択肢Aは誤りです。前述の通り、BCRは中小企業ではなく、大規模で複雑な企業に推奨されます。選択肢Bは誤解を招く記述です。SCCに関しては、データ輸出者がEU域外に所在してもよいと示唆していますが、これは事実です。しかし、BCRとの比較には関係ありません。なぜなら、データ輸出者は、GDPR第3条第2項に基づきGDPRの対象となる限り、BCRに関してもEU域外に所在することができるからです。選択肢Dも誤解を招く記述です。SCCを締結するためには、すべてのEUデータ保護当局の事前承認が必要であると示唆していますが、これは誤りです。SCCが追加の条項や保護措置によって修正または補足されない限り、企業はデータ輸出者が所在する加盟国の管轄監督当局の事前承認のみを必要とするからです。参考：
1: [GDPR第44条]
2: [GDPR第45条]
3: [GDPR第46条]
4: [GDPR第4条（20）]
5: [GDPR第47条]
6: [GDPR第63条]
7: [GDPR第93条]
8: [GDPR第46条(2)および(d)]
9: [拘束的企業準則（BCR）]
10: [GDPR第3条(2)]
11: [GDPR第46条(3)(a)および(b)]
12: [個人データの処理に関する自然人の保護及びそのようなデータの自由な移動に関する2016年4月27日の欧州議会及び理事会の規則（EU）2016/679、並びに指令95/46/ECの廃止（一般データ保護規則）]
13: [拘束的企業準則（BCR）- 欧州委員会]
14: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679]
15: [https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en]
16: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679]
17: [https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en]

最新問題**: 244**
シナリオ
次の質問に答えるには、以下を使用してください。

ハビエルはフィットネスクラブEVERFITの会員です。この会社は多くのEU加盟国に支店を持っていますが、GDPRの目的上、主要な事業所はフランスにあります。ハビエルは北アイルランドのニューリー（英国の一部）に住んでおり、国境を越えてアイルランドのダンドークに通勤しています。2年前、出張中にドイツのフランクフルトにあるEVERFITの支店でトレーニングをしているところを写真に撮られました。当時、ハビエルは写真がプロモーション目的のみに使用されることを伝えられ、写真に写ることに同意しました。それ以来、この写真はクラブの英国支部で使用されています。
パンフレットにも掲載され、英国ウェブサイトのランディングページにも掲載されています。しかし、このフィットネスクラブは最近、EU加盟国にある複数の支店で会員への不当な扱いが蔓延したため、評判が悪化しています。そのため、ハビエルさんは自分の写真がフィットネスクラブと公に結び付けられることに抵抗を感じています。
この件について話し合うため、地元支店の支店長との面談予約を何度も試みたものの、うまくいかなかったハビエルはEVETFITに手紙を送り、ウェブサイトとすべての販促資料から自分の写真を削除するよう要請した。数ヶ月が経過しても、要請に対する返答がなかったハビエルは、この件について強い不安を抱くようになった。他の手段を用いてEVETFITに何度も連絡を取ろうとしたが、それでもうまくいかなかったため、彼はEVETFITに対して訴訟を起こすことを決意した。
ハビエルは、この件について苦情を申し立てるため、英国情報コミッショナー事務局（ICO）に連絡した。ICOは、GDPR第56条（3）に基づき、CNIL（すなわち、
この問題に関して、EVERFITの主要拠点の監督機関であるCNILに連絡を取った。EVERFITは英国に拠点があるにもかかわらず、CNILは第10条に基づいて本件を処理することを決定した。
GDPR第60条に基づき、CNILは協力手続きに基づきICOと連携します。監督当局間の決定における問題を考慮し、欧州データ保護会議（European Data Protection Board）が関与し、一貫性メカニズムに基づき拘束力のある決定を下します。
さらに、ハビエルさんは、パンフレットとウェブサイトから自分の写真を削除するという要求をEVERFITが受け入れなかったことによる損害についてEVERFITを訴えている。
複数の EU 諸国にわたる複数の EVETFIT 支部が別々のデータ管理者として機能し、各支部が Javier の要求を不適切に処理した責任があると仮定した場合、Javier は補償を求めるためにどのような手続きを取ることができますか?
A. 彼は、EVETFIT の主要拠点があるフランスにある EVETFIT 本社を訴える必要があるでしょう。
B. 各支部が全損害に対して責任を負う可能性があるため、彼は関連する EVETFIT 支部のいずれかを訴えることができます。
C. ハビエルは、各 EVETFIT 支部を訴えて、各支部がハビエルが被った損害や苦痛への貢献度に応じて比例した補償金を支払うようにしなければなりません。
D. 彼は、欧州データ保護委員会の決定に基づいて、どの EVETFIT 支部が損害賠償責任を負うのかを決定するために、欧州データ保護委員会に申請することができます。
Answer: (解答を表示する**)**
GDPR第82条1によれば、GDPR違反の結果として物質的または非物質的な損害を被った者は、管理者または処理者から損害賠償を受ける権利を有します。処理に関与する管理者は、GDPRに違反する処理によって生じた損害について責任を負います。複数の管理者または処理者、あるいは管理者と処理者の両方が同一の処理に関与し、処理によって生じた損害について責任を負う場合、データ主体への効果的な賠償を確保するため、各管理者または処理者は損害の全額について責任を負うものとします。したがって、ハビエルは、自身の同意なしに、かつ自身の権利を侵害して個人データを処理したEVETFITのいずれかの支部を訴え、その支部に対して全額の賠償を請求することができます。賠償金を支払った支部は、同一の処理に関与した他の支部に対して、損害に対する各自の責任に相当する賠償金の返還を請求することができます。参考文献：GDPR第82条1項 - 賠償および責任の権利
- General Data Protection Regulation (GDPR)

最新問題**: 245**

フランスの管理者がモロッコ、アルジェリア、チュニジアでのみ利用可能なカーシェアリング アプリを所有しているが、データ処理活動がスペインの指定処理者によって実行される場合、次の条件を満たす限り、個人データの処理に GDPR が適用されますか?
A. データ処理活動はスペインで行われます。
B. 当該個人は欧州市民または居住者です。
C. データ管理者はフランスにいます。
D. EU の個人がターゲットになります。
Answer: D (メーッセージを残す)

最新問題: **246**
シナリオ
次の質問に答えるには、以下を使用してください。
ジョーは2000年、米国バーモント州の自宅でグミベア ・カンパニーを設立しました。現在、同社は数十億ドル規模のキャンディ会社に成長し、全大陸で事業を展開しています。同社のITサーバーはすべてバーモント州に設置されています。今年、ジョーは息子のベンを会社に迎え入れ、わずか5年で総売上高を3倍にするという大規模なマーケティング戦略 「プロジェクト ・ビッグ」の責任者に任命しました。ベンは一流大学でコンピュータ ソフトウェアの博士号を取得しています。ベンは父親の会社に加わることを決めましたが、同時に 「ベン ・ノウズ ・ベスト」という新しいグローバルオンラインデートサイト会社の立ち上げにも密かに取り組んでいます。
ベンは、グミベア ・カンパニーが何百万人もの顧客を抱えていることを認識しており、その多くが理想のパートナーを見つけることに興味を持っているかもしれないと考えています。プロジェクト ・ビッグでは、ベンは同社のオンライン ・ウェブポータルを再設計し、EUおよびその他の地域の顧客に、顧客維持のために追加の個人情報の提供を求めます。プロジェクト ・ベンは、顧客の哲学的信条、政治的意見、婚姻状況に関するデータの収集を開始します。
顧客が独身の場合、ベンはその顧客の個人データをすべてベン ・ノウズ ・ベストの別のデータベースにコピーします。ベンは、顧客一人ひとりに情報提供前にチェックボックスにチェックを入れるよう明確に同意を求めているため、何も悪いことはしていないと考えています。プロジェクト ・ビッグは重要なプロジェクトであるため、ベンの支援のため、コンピューターサイエンスを専攻する大学1年生のサムも採用しています。
ベンが声をかけると、サムはベン ・ノウズ ・ベストのデータベースを見つける。サムは10人の友人とスプリング ・ビーク号でアイルランドへ行く予定なので、アイルランド在住の顧客情報をすべてコピーして、アイルランド滞在中に友人と連絡が取れるようにする。
ジョーは、親友の娘でアメリカのロースクールを卒業したばかりのアリスを、会社の新しい法務顧問として採用しました。アリスはGDPRについて聞いていたので、調べてみました。そしてジョーに近づき、EU域内の事業所から米国への社内データ転送のための法的メカニズムを整備することが会社にとって重要であるため、会社全員が遵守すべき拘束的企業準則（BCR）を起草したと伝えました。
ジョーはアリスの素晴らしい仕事ぶりを高く評価し、米国連邦裁判所で会社に対して提起された大規模な訴訟の処理もアリスに任せると伝えた。訴訟に備えるため、アリスは会社のIT部門に指示し、EUを含む全世界の営業チームのコンピューターのハードドライブのコピーを作成し、全てをアリスに送ってもらい、全員の情報を確認できるようにする。アリスは、自分が第一段階のレビューを担当してくれたことで、ジョーはきっと喜ぶだろうと確信している。なぜなら、これにより、本来であれば外部の法律事務所に支払うはずだった多額の費用を節約できるからだ。
ベンが顧客から追加データを収集したことで、会社にいくつかの潜在的な問題が発生しましたが、おそらく何が必要になるでしょうか?
A. 新しい企業統治と行動規範。
B. データ保護影響評価。

C. 包括的なデータ インベントリ。
D. データ保護責任者の雇用。
Answer: B (メーッセージを残す**)**
ベンが顧客から追加データ、特に哲学的信念や政治的意見などの機密データを収集したことで、会社にとって次のようないくつかの潜在的な問題が生じました。
収集される個人データは適切かつ関連性があり、処理の目的に必要なものに限定される必要があることを要求するデータ最小化の原則に違反するリスク1。
データ主体が Ben Knows Best によるデータの二次利用、または Sam によるデータへの不正アクセスやコピーを認識していない、または同意していない可能性のある、データ主体の権利と自由を侵害するリスク。
GDPRの特別なカテゴリーのデータ処理要件に違反するリスク。これには哲学的信念や政治的意見を明らかにするデータが含まれます。このようなデータは、明示的な同意、相当な公共の利益、法的請求など、特定の条件下でのみ処理できます2。
データが別のデータベースに転送され、サムによってコピーされ、適切なセキュリティ対策や安全対策が施されていない可能性のあるバーモント州にある会社のサーバーに保存されるため、データ漏洩や損失のリスクがあります。
したがって、企業はこれらのリスクを特定し、軽減するために、データ保護影響評価（DPIA）を実施する可能性が最も高いでしょう。DPIAとは、想定される処理業務が個人データ保護に与える影響を評価し、DPIAの結果、管理者がリスク軽減措置を講じない場合、処理によって高いリスクが生じると判断された場合、監督機関に相談するプロセスです3。その他の選択肢は、GDPRで必ずしも義務付けられているわけではありませんが、グッドプラクティスや契約条件として挙げられる場合があります。参考：
無料のCIPP/E学習ガイド、32ページ、セクション4.1.2
CIPP/E認証、27ページ、セクション4.1.2
2023年版CIPP/E究極学習ガイド、36ページ、セクション4.1.2
原則 - 一般データ保護規則（GDPR）第5条
個人データの特別なカテゴリ - 一般データ保護規則（GDPR）第9条 データ保護影響評価 - 一般データ保護規則（GDPR）第35条

最新問題**: 247**
GDPR では、個人データがデータ主体から直接取得されない場合、次の条件を満たす場合、管理者はデータ処理に関する情報をデータ主体に直接提供することが免除されます。
A. データ主体は、自分のデータがどのように使用されるかについてすでに情報を持っている
B. データ主体にそのような情報を提供することはあまりにも問題が多い
C. 第三者のデータは、データ主体に情報を提供することで開示される。
D. データ主体のデータの処理は適切な技術的手段によって保護されている
Answer: A (メーッセージを残す**)**
説明/参照: https://dataprivacymanager.net/gdpr-exemptions-from-the-obligation-to-provide-information-to-the- individual-data-subject/

最新問題**: 248**
次の手順をお読みください。
* どの従業員がどのデバイスやアプリからクラウドサービスにアクセスしているかを把握し、それらのアプリやデバイスのデータをロックダウンします。
* アプリとデバイスのコンプライアンスを監視および分析する
* アプリケーションのライフサイクルを管理する

* データ共有を監視する
組織は次のどれを実行するためにこれらの手順を実行する必要がありますか?
A. GDPR に準拠した Privacy by Design プロセスを追求します。
B. GDPR に準拠した従業員監視プロセスを導入します。
C. 安全な Bring Your Own Device (BYOD) プログラムを維持します。
D. クラウドベンダーが社内データ使用ポリシーに準拠していることを確認します。
Answer: (解答を表示する**)**
質問に記載されている手順は、従業員が個人のデバイスを使用して組織のデータやアプリケーションにアクセスできるようにする安全な BYOD プログラムを実装するためのベスト プラクティス フレームワークの一部です。
BYODプログラムは、データ漏洩、不正アクセス、マルウェア感染、コンプライアンス違反など、プライバシーとセキュリティに関する重大なリスクをもたらします。そのため、組織はBYODプログラムに関連するデバイス、アプリ、データの検出、監視、管理、セキュリティ確保のための包括的なアプローチを採用する必要があります。
このアプローチは、組織が設計段階およびデフォルト設定によるデータ保護、データセキュリティ、アカウンタビリティ、データ侵害通知に関するGDPR要件を満たすのに役立ちます。参考資料：
* 無料のCIPP/E学習ガイド、15ページ、セクション2.3.3
* CIPP/E認証、10ページ、セクション1.1.2
* Cipp-e 学習ガイド、授業ノートと要約、 ‘CIPP/E 試験概要 2023」文書、42 ページ、セクション 2.3.3

最新問題**: 249**
スペインのデータ保護局が最近採用した個人データ保護委員会 (PDPC) の 基本的なデータ匿名化技術に関するガイド」によると、次のどれが有効な基本的な匿名化技術ではないでしょうか。
A. スワッピング。
B. 一般化。
C. データ調整。
D. 属性の抑制。
Answer: (解答を表示する**)**
PDPCのガイド12によると、データ調整は有効な基本的匿名化手法ではありません。データ調整とは、ランダムな量を加算または減算したり、ランダムな係数を乗算または除算したりすることで、元のデータ値を変更することを指します3。この手法はデータの統計特性の一部を維持する可能性がありますが、データの有用性や品質に影響を与える可能性のあるエラーや不正確さも生じます3。さらに、調整されたデータは他のデータソースとリンクまたは照合される可能性があるため、データ調整では個人の身元を十分に保護できない可能性があります3。したがって、PDPCはデータ調整を基本的匿名化手法として推奨していません。
参照：
1: 基本的なデータ匿名化技術ガイド 2018年1月25日発行 - PDPC 2: 基本的な匿名化ガイド - PDPC 3: PDPCからの無料ツールと基本的な匿名化ガイド

最新問題**: 250**
プライバシーおよび電子通信規制（指令2002/58/EC）の規定に最も含まれないマーケティング関連活動はどれですか?
A. ウェブサイトに受動的に表示される広告。
B. 個人に関するデータを収集するためにクッキーを使用すること。

C. コンサートチケットを販売している会社から個人に送られるテキストメッセージ。
D. 小売店が以前の顧客にセールを宣伝するメール。
Answer: A (メーッセージを残す**)**
プライバシーおよび電子通信規則（PECR）は、電子プライバシー指令から派生したものである。
2002/58/ECは、電子通信サービスの利用者のプライバシーと機密性を保護することを目的としています。PECRは、Cookieの使用、迷惑通信、トラフィックデータや位置情報データなど、電子マーケティングの様々な側面を規定しています。PECRによれば、以下のマーケティング関連活動は、特定の例外が適用される場合を除き、利用者または加入者の同意を必要とします。
* ユーザーのデバイスに情報を保存したり、情報にアクセスしたりするために Cookie または同様のテクノロジーを使用する (規則6)。
* 事前の同意を得ていない個々の加入者にダイレクトマーケティングの目的で電子メールを送信すること（規則22）。
* 電話優先サービスに自分の番号を登録した個人加入者、または特定の発信者からのそのような電話を拒否した個人加入者に対して、ダイレクトマーケティングの目的で迷惑電話をかけること（規則21）。
* 法人加入者がそのような通信を受信したくないと表明していない限り、電子メール、ファックス、または自動通話システムを使用してダイレクトマーケティングの目的で迷惑な通信を法人加入者に送信すること（規則23）。
したがって、4つの選択肢のうち、PECRの規定の適用範囲が最も狭いのは、ウェブサイトに受動的に表示される広告です。これは、Cookieの使用、迷惑メッセージの送信、トラフィックデータや位置情報データの処理を伴わないためです。ただし、このような広告は、ユーザーの個人データの処理を伴う場合、GDPRなどの他のデータ保護法の対象となる可能性があります。
参考文献:
ペック
電子プライバシー指令
PECRに関するICOガイド
参考: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02002L0058-20091219&from=RO

最新問題**: 251**
一般データ保護規則 (GDPR) と欧州評議会条約 108 の両方に当てはまるものは何ですか?
A. どちらも欧州連合諸国にのみ適用されます
B. どちらも個人データの国際転送を規制しています
C. どちらも個人データの手動処理を規定しています
D. どちらも、処理活動の監督機関への通知が必要です。
Answer: D (メーッセージを残す**)**

最新問題**: 252**
次のすべては、第 2 次ネットワークおよび情報セキュリティ指令（「NIS2」) によって確立されますが、次のものを除きます。
A. 対象となる各エンティティが対処しなければならないベースラインのサイバーセキュリティ対策。
B. 対象となる組織を検査、監査、または情報を要求する権限。
C. A common controls framework that every organization must adopt.
D. A new network for EU member states to cooperate on large-scale breaches.
Answer: C (メーッセージを残す**)**

The NIS2 Directive is the EU's legislation on cybersecurity that updates and replaces the previous NIS Directive. It aims to create a high common level of cybersecurity across the EU by setting up legal measures for the security of network and information systems used by essential and important entities in various sectors and by enhancing cooperation among the member states. The NIS2 Directive does not establish a common controls framework that every organization must adopt, but rather allows each member state to define the appropriate security measures and incident reporting requirements for the entities under its jurisdiction, taking into account the specificities of each sector and subsector. However, the NIS2 Directive does provide some general principles and objectives for the security measures, such as proportionality, risk-based approach, state of the art, and regular review and update. The NIS2 Directive also introduces minimum harmonised rules for the supervision and enforcement of the security measures and incident reporting obligations, including the possibility of imposing administrative fines.
References:
NIS2 Directive, Articles 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, and 14.
The NIS2 Directive: A high common level of cybersecurity in the EU, pages 1, 2, 3, 4, 5, 6, 7, and 8.

最新問題**: 253**
データ侵害によって生じるリスクのレベルを評価する際に、考慮する必要がないのは次のどれですか?
A. 個人の識別の容易さ。
B. 関係するデータ プロセッサのサイズ。
C. データ コントローラーの特殊な特性。
D. 個人データの性質、機密性、量。
Answer: B (メーッセージを残す**)**
データ侵害によって生じるリスクのレベルを評価する際に、関与するデータ処理者の規模を考慮する必要はありません。GDPRによれば、データ侵害とは「送信、保管、またはその他の方法で処理された個人データの偶発的または違法な破壊、紛失、改ざん、不正開示、またはアクセスにつながるセキュリティ侵害」です1。GDPRは、データ管理者およびデータ処理者に対し、データ侵害が自然人の権利と自由にリスクをもたらす可能性が低い場合を除き、72時間以内に関連監督機関にデータ侵害を通知することを義務付けています2。また、GDPRは、データ侵害がデータ主体の権利と自由に高いリスクをもたらす可能性がある場合、データ管理者に対し、影響を受けるデータ主体にデータ侵害を遅滞なく通知することを義務付けています3。
GDPRはリスクレベルを判断するための具体的な基準を明示していませんが、前文85において「データ主体の権利と自由に対するリスクの可能性と重大性は、処理の性質、範囲、状況、目的を参照して判断されるべきである」という指針を示しています。また、前文では、個人の識別の容易さ、個人データの特殊なカテゴリ、処理の大規模さ、データ管理者の特殊な特性など、リスクを高める可能性のある要因についても言及しています。したがって、データ侵害によって生じるリスクレベルを評価する際には、これらの要因を考慮する必要があります。
ただし、関係するデータ処理者の規模は、データ主体に対する侵害の影響に影響を与えないため、リスク評価には関係ありません。データ処理者は、データ管理者に代わって個人データを処理する責任のみを負い、データ主体とは直接の関係を持ちません。データ侵害が発生した場合のデータ処理者の義務は、データ管理者に遅滞なく通知すること、およびデータ管理者が GDPR に基づく義務を遵守できるよう支援することです。データ処理者の規模は、これらの義務を履行する能力に影響を与える可能性がありますが、データ侵害自体によって生じるリスクのレベルは変わりません。参考文献 : 1: GDPR 第 4 条 (12) 2: GDPR 第 33 条 3: GDPR 第 34 条
GDPR 序文第85条 :GDPR 第4条(8)項 :GDPR 第28条 以上がお役に立てれば幸いです。他にご質問がございましたら、お気軽にお問い合わせください。#

最新問題: **254**
GDPR第4条(22)が 関係監督当局」の概念を確立した主な理由は何ですか?
A. ローカル データ処理アクティビティの一貫性を促進します。
B. 企業に監督機関を誰にするか選択する権利を与える。
C. EU 内に拠点がないが、加盟国に代表者を持つ管理者にも GDPR が適用されるようにします。
D. 主導機関の管轄区域外に居住する個人の利益が代表されるようにする。
Answer: D (メーッセージを残す)
GDPR第4条22項によれば、監督機関は、その加盟国に居住するデータ主体が個人データの処理によって実質的に影響を受けている、または影響を受ける可能性がある場合、あるいは苦情が申し立てられている場合、個人データの処理について関係機関とみなされます。この概念は主に、管理者または処理者の所在地や主たる監督機関の所在地に関わらず、データ主体の権利と利益が最も近い監督機関によって保護されることを確保するために導入されました。関係監督機関は、ワンストップショップメカニズムおよび一貫性メカニズムに参加する権利、および主たる監督機関の決定案に対する意見や異議を表明する権利を有します。また、それぞれの任務の遂行において、相互に協力し、支援する義務を負います。参考文献 :GDPR第4条22項、GDPR第60条、GDPR第63条、 関係監督機関」の役割（第3.1章）...

最新問題: **255**
GDPR の第 4 条 (5) に基づき、データが 仮名化」されているとみなされるのは次の場合ですか?
A. 第三者によってのみ人物に帰属させることができます。
B. 追加情報を使用せずにデータ主体に帰属させることはできません。
C. いかなる状況においても、個人に帰属させることはできません。
D. コントローラーによってのみ人物に帰属させることができます。
Answer: B (メーッセージを残す)

最新問題: **256**
シナリオ
次の質問に答えるには、以下を使用してください。
サンディは最近、2016年に設立された広告テクノロジー企業Market4Uにプライバシーおよびデータガバナンス担当バイスプレジデントとして入社しました。データインベントリの実施という最初の取り組みを通して、サンディはMarket4Uが設立以来収集してきた1,900万人のグローバル連絡先リストを保有していることを知りました。膨大なデータ量のリスクを認識していたサンディは、2018年5月以前にMarket4Uのシステムに入力された連絡先のうち、Market4Uのコンテンツに最近アクセスした連絡先を除いて、すべて削除したいと考えていました。しかし、営業担当バイスプレジデントのダンは、すべての連絡先がMarket4Uのクライアントにとって、成功したマーケティングキャンペーンや業界動向に関する有用な情報を提供しているとサンディに伝えました。
ダンはサンディに、スポーツ ・エンターテイメント業界の顧客獲得に注力したいと伝えました。この顧客獲得を支援するため、Market4Uのマーケティングチームは、Market4Uのウェブサイトフォームに、ホワイトペーパーのダウンロード、Market4Uフォーラムへの参加用アカウント作成、イベントへの参加など、いくつかの新しいフィールドを追加することにしました。これらのフィールドには、生年月日や給与などが含まれています。
ダンが Market4U のフォームに追加したい新しいフィールドに関して、サンディはダンとマーケティング チームにどのようなフィードバックを与えるべきでしょうか?

A. すべてのフィールドをオプションにします。
B. 括弧内の情報のみを要求します (年齢層や給与範囲など)。
C. フィールドは提供されるサービスに比例していないため、削除します。
D. ホワイトペーパーの提供やイベントの登録の目的には必要ないので、フィールドを削除します。
Answer: D (メーッセージを残す)
サンディはこのフィードバックをダンとマーケティングチームに伝えるべきです。これはデータ最小化の原則を反映しており、収集される個人データは適切かつ関連性があり、処理目的に必要な範囲に限定される必要があるとされています1。ホワイトペーパーのダウンロードやイベントへの登録を希望する顧客から生年月日や給与情報を収集することは、これらの目的には不要であり、データ保護とセキュリティにリスクをもたらす可能性があります。さらに、このような情報は、データ主体からの明示的な同意が必要であり、特定の条件下でのみ処理できる特別なデータに該当する可能性があります2。その他の選択肢は、たとえ任意または括弧内であっても、必要以上のデータを収集することになるため、データ最小化の原則に準拠していません。参考：
無料のCIPP/E学習ガイド、23ページ、セクション3.1
CIPP/E認証、18ページ、セクション3.1
2023年版CIPP/E究極学習ガイド、16ページ、セクション3.1
原則 - 一般データ保護規則（GDPR）第5条
個人データの特別なカテゴリ - 一般データ保護規則（GDPR）第9条

最新問題: **257**
GDPR第80条(1)に基づき、個人はプライバシーに関する集団訴訟またはクラスアクションにおいて、非営利団体を代理人として選任することができます。これらの団体は一般的に何と呼ばれていますか？
A. 法律事務所組織。
B. 市民社会組織。
C. 人権団体。
D. 憲法上の権利団体。
Answer: B (メーッセージを残す)
GDPR の第 80 条 (1) は、データ主体は、加盟国の法律に従って適切に設立され、公共の利益となる法定目的を持ち、個人データの保護に関するデータ主体の権利と自由の保護の分野で活動している非営利団体、組織、または協会に、自身に代わって苦情を申し立てること、自身に代わって第 77 条、第 78 条、および第 79 条で言及される権利を行使すること、および自身に代わって第 82 条で言及される補償を受ける権利を行使することを委任する権利を有すると規定しています1。これらの非営利団体、組織、または協会は、公共の場で市民やグループの利益を代表するため、一般に市民社会組織と呼ばれています2。その他の選択肢は、次の理由により正しくありません。(A) 法律事務所組織は必ずしも非営利またはデータ保護の分野で活動しているわけではありません。人権団体は市民社会組織のサブセットですが、すべての市民社会組織が人権に焦点を当てているわけではありません。(D) 憲法上の権利を擁護する団

体も市民社会団体の一部ですが、すべての市民社会団体が憲法上の権利に関心を持っているわけではありません。参考文献 :1 :GDPR第80条(1)、2：無料のCIPP/E学習ガイド、48ページ。

最新問題**: 258**
SCENARIO
Please use the following to answer the next question:
Brady is a computer programmer based in New Zealand who has been running his own business for two years. Brady's business provides a low-cost suite of services to customers throughout the European Economic Area (EEA). The services are targeted towards new and aspiring small business owners. Brady's company, called Brady Box, provides web page design services, a Social Networking Service (SNS) and consulting services that help people manage their own online stores.
Unfortunately, Brady has been receiving some complaints. A customer named Anna recently uploaded her plans for a new product onto Brady Box's chat area, which is open to public viewing. Although she realized her mistake two weeks later and removed the document, Anna is holding Brady Box responsible for not noticing the error through regular monitoring of the website. Brady believes he should not be held liable.
もう一人の顧客、フェリペは、自分の個人情報がHermes Designsというサードパーティの請負業者に転送されたことを知って驚き、自分のビジネス計画に関する機密情報が悪用されるのではないかと心配しています。ブレイディは、欧州のプライバシー規則に違反したとは思っていません。彼は、要求されたサービスの履行において個人データが特定のサードパーティに転送される可能性があることを明示的に記載したプライバシー通知をすべての顧客に提供しています。フェリペはプライバシー通知を読んだが、長くて複雑だったと言います。ブレイディは、Hermes Designsの誠実さを個人的に保証できるため、フェリペが心配する必要はないと主張し続けています。実際、Hermes Designsは、フェリペのような顧客のために、カスタマイズされたバナー広告のサンプルを作成することを率先して行っています。ブレイディは、現在Hermes DesignsのWebページに掲載されているサンプルバナー広告へのリンクを喜んで提供します。Hermes Designsは、これらの顧客へのダイレクトマーケティングをフォローアップする予定です。
ブレイディ氏は、別の顧客であるセルジュ氏から、自身の発言がブレイディボックスのホームページ上のグラフィックコラージュに使用されていることに憤慨していると伝えられ、驚きました。この発言はセルジュ氏の名前で表記されています。しかし、ブレイディ氏は訴訟を懸念していませんでした。セルジュ氏に返信し、この発言はブレイディボックスのソーシャルネットワーキングサービス（SNS）で見つけたと伝えました。セルジュ氏自身がこの発言を投稿したからです。返信の中で、ブレイディ氏は礼儀として発言を削除することを申し出ました。
顧客からの苦情はあるものの、ブレイディ氏のビジネスは好調だ。彼は、明確な役割分担を定めたサードパーティの広告ネットワークを通じたオンライン行動ターゲティング広告（OBA）で収入を補っている。
ブレイディ氏は、一部の顧客が OBA を明確に認識していないにもかかわらず、広告に有用な製品やサービスが含まれていることを喜んでいます。
欧州のプライバシー慣行の現在の傾向に基づくと、Brady Box が欧州に進出した場合、同社のオンライン行動ターゲティング広告 (OBA) のどの側面が不十分になる可能性が高いでしょうか。
A. オプトインのオプションがない。
B. ウェブサイト内のセキュリティのレベル。
C. サードパーティの広告ネットワークとの契約。
D. 広告の内容が承認される必要がある。
Answer: (解答を表示する**)**
オンライン行動広告（OBA）とは、特定のコンピュータまたはデバイスから、ウェブ閲覧行動に関するデータを、共通の管理下にない複数のウェブドメインにわたって、経時的に収集することを指します。そのデータを使用してウェブユーザーの嗜好や興味を予測

し、そのウェブ閲覧行動から推測される嗜好や興味に基づいて、特定のコンピュータまたはデバイスにオンライン広告を配信することを目的としています1。OBAは、個人データ処理への同意に関するEU法の対象であり、データ主体による処理への同意を示す明確な肯定的行動が求められます2。同意は、自由意志によるものであり、具体的で、十分な情報に基づいたものであり、曖昧さがなく、いつでも撤回できます2。また、OBAの目的でデータを収集および使用する前に、同意を得る必要があります3。したがって、Brady BoxのOBAの実践は、

最新問題: **259**
シナリオ
次の質問に答えるには、以下を使用してください。
アンナとフランクは二人ともグランチェスター大学で働いています。アンナはデータ保護を担当する弁護士で、フランクは工学部の講師です。大学では様々な種類の記録を保管しています。
* 学生記録には、氏名、学生番号、自宅住所、大学入学前の情報、大学の出席および成績記録、特別な教育ニーズの詳細、財務情報が含まれます。
* 自伝的資料（カリキュラム、専門家の連絡先ファイル、学生の評価、その他の関連する教育ファイルなど）を含むスタッフの記録。
* 卒業生の記録（出身地、生年、入学日、学位授与日など）。
これらの記録は、グランチェスターの卒業生ポータルに登録した卒業生が閲覧できます。
* 教育省の記録。特定の人口統計グループ（第一世代の生徒など）の平均的な進級見込みを示しています。これらの記録には、氏名や身分証明書番号は含まれていません。
* 大学はセキュリティ ポリシーに従い、転送中および保存中のすべての個人データ記録を暗号化します。
フランクは、教育の質を向上させるため、工学部の学生の成績が教育省の期待値とどの程度一致しているかを調査したいと考えています。彼はアンナのデータ保護研修コースを受講しており、目標達成に必要な範囲を超えて個人データを使用するべきではないことを理解しています。そこで、学生の過去出身校、当初の成績、現在の成績、初めて進学した大学など、一部のデータのみをエクスポートするプログラムを作成しました。記録は個々の学生レベルで保存したいと考えています。
フランクはアンナの訓練を踏まえ、生徒番号をアルゴリズムにかけ、異なる参照番号に変換します。彼は毎回同じアルゴリズムを使用することで、時間の経過とともに各記録を更新していきます。
アンナの業務の一つは、GDPRの要件に従い、処理活動の記録を完了することです。GDPRの要件に従い、アンナからメールによるリマインダーを受け取った後、フランクはアンナにパフォーマンスデータベースについて連絡します。
アンはフランクに、個人データを最小限に抑えるだけでなく、大学は既存データの新たな利用が許容されるかどうかを確認する必要があると説明した。また、GDPRの下では、データ処理を実施する前にリスク分析を実施する必要があるのではないかとも考えている。アンナは追加調査を行った後、フランクとこの件についてさらに話し合う予定だ。
フランクは空き時間に分析作業を行いたいと考え、データを自宅のノートパソコン（暗号化されていない）に転送しました。ところが、大学にノートパソコンを持っていく途中、電車の中で紛失してしまいます。その日、フランクは互換性のある処理について話し合うため、アンナと面会する必要がありました。セキュリティインシデントを報告する必要があるため、同時にアンナにもノートパソコンの紛失について伝えることにしました。
アンナがフランクのパフォーマンス データベースが許可されるかどうかを判断する前に、どのような追加情報が必要ですか?
A. 学生に伝えられた内容と研究がどのように使用されるかについての詳細情報。
B. 情報損失の範囲に関する詳細情報。
C. フランクが学生番号を隠すために使用したアルゴリズムの詳細情報。
D. Frank のデータ保護トレーニングに関する詳細情報。

Answer: A (メーッセージを残す)

最新問題: **260**
スペインに拠点を置き、世界中でドキュメンタリーを撮影する著名なビデオ制作会社が、マドリードの街頭で高齢者を撮影した数時間分の映像を収録し終えたばかりです。どのような条件であれば、ドキュメンタリーに使用する画像を使用するすべての人から同意を得る必要がないのでしょうか？
A. 同意を得るのに過度の労力がかかると判断された場合。
B. 同意を得ることが現地の法律によって任意であるとみなされる場合。
C. 企業が映像を法定年齢に達したデータ主体のみに限定している場合。
D. 企業がドキュメンタリープロバイダーとしての地位により正当な利益を主張できる場合。
Answer: (解答を表示する)
GDPRによれば、同意は個人データ処理の6つの法的根拠の一つですが、唯一の根拠ではありません。他の5つは、契約、法的義務、重要な利益、公的任務、そして正当な利益です。正当な利益は、個人データを自らの利益または第三者の利益のために処理する管理者によって主張することができます。ただし、当該処理がデータ主体（特に未成年者）の権利と自由を侵害しない限りにおいてです。GDPRはまた、ジャーナリズム目的、または学術的、芸術的、もしくは文学的表現の目的で個人データを処理することが、正当な利益である表現の自由および情報の自由の権利の行使に必要となる場合があることも認めています。したがって、企業は、ジャーナリズム、芸術的、もしくは文学的表現の目的において処理が必要であること、そしてデータ主体の合理的な期待とプライバシーへの潜在的な影響を考慮していることを実証できる場合、ドキュメンタリーに使用する画像のすべての人物から同意を得る必要がない可能性があります。また、企業は、当該処理に適用される可能性のある関連する国内法または行動規範を遵守する必要があります。
参考：
GDPR第6条(1)(a)-(f)
GDPR、前文47
GDPR第85条